

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-77131

(P2002-77131A)

(43)公開日 平成14年3月15日(2002.3.15)

(51)Int.Cl.⁷

H 0 4 L 9/08

識別記号

F I

H 0 4 L 9/00

キーワード(参考)

6 0 1 B 5 J 1 0 4

6 0 1 A

審査請求 未請求 請求項の数30 O L (全 49 頁)

(21)出願番号 特願2000-317803(P2000-317803)

(22)出願日 平成12年10月18日(2000.10.18)

(31)優先権主張番号 特願2000-105329(P2000-105329)

(32)優先日 平成12年4月6日(2000.4.6)

(33)優先権主張国 日本(J P)

(31)優先権主張番号 特願2000-179692(P2000-179692)

(32)優先日 平成12年6月15日(2000.6.15)

(33)優先権主張国 日本(J P)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 石黒 隆二

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 大澤 義知

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74)代理人 100101801

弁理士 山田 英治 (外2名)

最終頁に続く

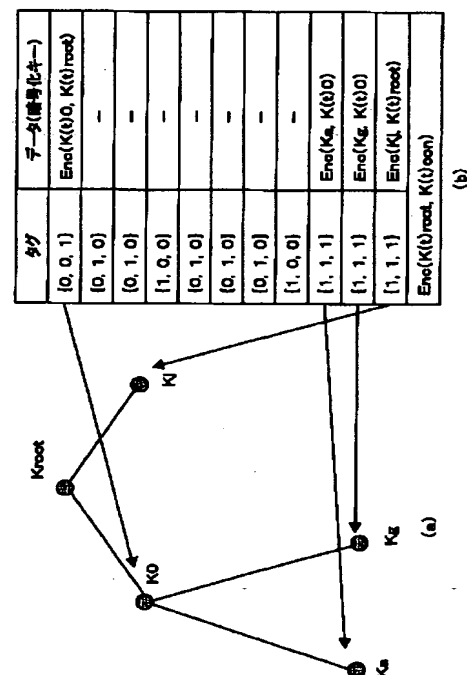
(54)【発明の名称】 情報処理システム、情報処理方法、および情報記録媒体、並びにプログラム提供媒体

(57)【要約】

【課題】 ツリー構造の暗号化キー構成に用いる有効化キーブロック(EKB)のデータ量の削減を可能とした情報処理システムおよび方法を実現する。

【解決手段】 ツリー構造のキー配布構成に用いる有効化キーブロック(EKB)を、復号可能な末端ノードまたはリーフを最下段として簡略化した2分岐または多分岐型ツリーを再構築して、再構築階層ツリーのノードまたはリーフに対応するキーのみに基づいて生成する。さらに、EKBに格納した暗号化キーのツリー位置の識別データとしてのタグを格納する。タグは、位置識別のみならず、EKB内の暗号化キーデータの有無を判別するデータを格納した構成とした。EKBの大幅なデータ量削減が実現するとともに、デバイスでの復号処理も簡易化される。

簡略化した暗号化キーブロック(EKB:Enabling Key Block)を用いた
デバイスKa、Kb、Kc、Kdへのバージョンハのコンテイングキー-選択処理



1

【特許請求の範囲】

【請求項 1】 1 以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータを配信する情報処理システムであり、

個々のデバイスは、

複数の異なるデバイスをリーフとした階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するとともに、デバイスに対して配信される前記暗号化メッセージデータについての復号処理を前記キーセットを使用して実行する暗号処理手段を有し、

前記デバイスに提供される暗号化メッセージデータは、前記階層ツリー構造の 1 つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した暗号化キーデータを含む有効化キープロック (EKB) の復号処理によって得られる更新ノードキーによって暗号化されたデータ構成であり、

前記有効化キープロック (EKB) は、前記暗号化キーデータによって構成されるデータ部と、該データ部に格納される暗号化キーデータの前記階層ツリー構造における位置識別データとしてのタグ部とを含む構成であることを特徴とする情報処理システム。

【請求項 2】 前記有効化キープロック (EKB) に含まれる前記暗号化キーデータは、前記階層ツリー構造を構成するノードキーを下位ノードキーまたは下位リーフキーを用いて暗号化したデータであり、

前記タグ部に格納される位置識別データは、前記有効化キープロック (EKB) に格納された 1 以上の暗号化キーデータ各々のノード位置の下位の左右ノードまたはリーフ位置の暗号化キーデータの有無を示すタグとして構成されていることを特徴とする請求項 1 に記載の情報処理システム。

【請求項 3】 前記有効化キープロック (EKB) に含まれる前記暗号化キーデータは、該有効化キープロック

(EKB) を復号可能な末端ノードまたはリーフを最下段とした簡略化した 2 分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーのノードまたはリーフに対応するキーのみに基づいて構成され、

前記タグ部に格納される位置識別データは、前記有効化キープロック (EKB) のタグに対応する暗号化キーの格納の有無を示すデータを含む構成であることを特徴とする請求項 1 に記載の情報処理システム。

【請求項 4】 前記有効化キープロック (EKB) に含まれる前記暗号化キーデータは、該有効化キープロック

(EKB) を復号可能な末端ノードまたはリーフを最下段とした簡略化した 2 分岐型ツリーを構成するパスを選

2

択して不要ノードを省略することにより再構築される再構築階層ツリーのノードまたはリーフに対応するキーのみに基づいて構成され、

前記タグ部に格納される位置識別データは、前記有効化キープロック (EKB) に格納された 1 以上の暗号化キーデータ各々のノード位置の下位の左右ノードまたはリーフ位置の暗号化キーデータの有無を示すタグと、該タグに対応する暗号化キーの格納の有無を示すデータを含む構成であることを特徴とする請求項 1 に記載の情報処理システム。

【請求項 5】 前記再構築階層ツリーは、共通要素を持つデバイスの部分集合ツリーとして定義されるエンティティの頂点ノードであるサブルートを選択して構成されるツリーであることを特徴とする請求項 4 に記載の情報処理システム。

【請求項 6】 前記有効化キープロック (EKB) に含まれる前記暗号化キーデータは、該有効化キープロック (EKB) を復号可能な末端ノードまたはリーフを最下段とした簡略化した多分岐型ツリーにおいて、前記末端ノードまたはリーフと、該多分岐型ツリーの頂点とを直接接続するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーの頂点ノードおよび末端ノードまたはリーフに対応するキーのみに基づいて構成され、

前記タグ部に格納される位置識別データは、前記有効化キープロック (EKB) のタグに対応する暗号化キーの格納の有無を示すデータを含む構成であることを特徴とする請求項 1 に記載の情報処理システム。

【請求項 7】 前記再構築階層ツリーは、簡略化した多分岐型ツリーを構成する頂点ノードと、簡略化したツリーを構成する末端ノードまたはリーフとを直接、接続した 3 以上の分岐を持つツリーであることを特徴とする請求項 6 に記載の情報処理システム。

【請求項 8】 前記デバイスにおける前記暗号処理手段は、

前記有効化キープロック (EKB) の前記タグ部のデータにより、前記暗号化キーデータを順次抽出して、復号処理を実行し、前記更新ノードキーを取得し、該取得した更新ノードキーにより前記暗号化メッセージデータの復号を実行する構成であることを特徴とする請求項 1 に記載の情報処理システム。

【請求項 9】 前記メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーであることを特徴とする請求項 1 に記載の情報処理システム。

【請求項 10】 前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする請求項 1 に記載の情報処理システム。

【請求項 11】 前記メッセージデータは、コンテンツのインテグリティ・チェック値 (ICV) 生成キーである

3

ことを特徴とする請求項 1 に記載の情報処理システム。

【請求項 1 2】前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする請求項 1 に記載の情報処理システム。

【請求項 1 3】前記メッセージデータは、プログラムコードであることを特徴とする請求項 1 に記載の情報処理システム。

【請求項 1 4】1 以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータを配信する情報処理方法であり、

複数の異なるデバイスをリーフとした階層ツリー構造の 1 つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した暗号化キーデータを含むデータ部と、該データ部に格納される暗号化キーデータの暗記階層ツリー構造における位置識別データとしてのタグ部とを含む有効化キープロック (EKB) を生成する有効化キープロック (EKB) 生成ステップと、

前記更新ノードキーによって暗号化したメッセージデータを生成してデバイスに対して配信するメッセージデータ配信ステップと、

を有することを特徴とする情報処理方法。

【請求項 1 5】前記情報処理方法は、さらに、前記階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するデバイスにおいて、前記暗号化メッセージデータについての復号処理を前記キーセットを使用して実行する復号処理ステップ、
を有することを特徴とする請求項 1 4 に記載の情報処理方法。

【請求項 1 6】前記有効化キープロック (EKB) 生成ステップは、

前記階層ツリー構造を構成するノードキーを下位ノードキーまたは下位リーフキーを用いて暗号化して前記暗号化キーデータを生成するステップと、

前記有効化キープロック (EKB) に格納される 1 以上の暗号化キーデータ各々のノード位置の下位の左右位置のノードまたはリーフ位置の暗号化キーデータの有無を示すタグを生成して前記タグ部に格納するステップとを含むことを特徴とする請求項 1 4 に記載の情報処理方法。

【請求項 1 7】前記有効化キープロック (EKB) 生成ステップは、

該有効化キープロック (EKB) を復号可能な末端ノードまたはリーフを最下段とした簡略化した 2 分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築階層ツリーを生成するステップと、

4

前記再構築階層ツリーの構成ノードまたはリーフに対応するキーのみに基づいて有効化キープロック (EKB) を生成するステップと、

前記有効化キープロック (EKB) のタグに対応する暗号化キーの格納の有無を示すデータを前記タグ部に格納するステップと、

を含むことを特徴とする請求項 1 4 に記載の情報処理方法。

【請求項 1 8】前記再構築階層ツリーを生成するステップは、

共通要素を持つデバイスの部分集合ツリーとして定義されるエンティティの頂点ノードであるサブルートを選択して実行されるツリー生成処理であることを特徴とする請求項 1 7 に記載の情報処理方法。

【請求項 1 9】前記有効化キープロック (EKB) 生成ステップは、

該有効化キープロック (EKB) を復号可能な末端ノードまたはリーフを最下段とした簡略化した多分岐型ツリーにおいて、前記末端ノードまたはリーフと、該多分岐型ツリーの頂点とを直接接続するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーを生成するステップと、

前記有効化キープロック (EKB) のタグに対応する暗号化キーの格納の有無を示すデータを前記タグ部に格納するステップと、

を含むことを特徴とする請求項 1 4 に記載の情報処理方法。

【請求項 2 0】前記再構築階層ツリーの生成ステップにおいて生成する再構築階層ツリーは、簡略化した多分岐型ツリーを構成する頂点ノードと、簡略化したツリーを構成する末端ノードまたはリーフとを直接、接続した 3 以上の分岐を持つツリーとして生成することを特徴とする請求項 1 9 に記載の情報処理方法。

【請求項 2 1】前記復号処理ステップは、

前記有効化キープロック (EKB) の前記タグ部に格納された位置識別データに基づいて前記データ部に格納された暗号化キーデータを順次抽出して順次復号処理を実行することにより前記更新ノードキーを取得する更新ノードキー取得ステップと、

前記更新ノードキーにより前記暗号化メッセージデータの復号を実行するメッセージデータ復号ステップと、
を含むことを特徴とする請求項 1 5 に記載の情報処理方法。

【請求項 2 2】前記メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーであることを特徴とする請求項 1 4 に記載の情報処理方法。

【請求項 2 3】前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする請求項 1 4 に記載の情報処理方法。

5

【請求項24】前記メッセージデータは、コンテンツのインテグリティ・チェック値（ICV）生成キーであることを特徴とする請求項14に記載の情報処理方法。

【請求項25】前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする請求項14に記載の情報処理方法。

【請求項26】前記メッセージデータは、プログラムコードであることを特徴とする請求項14に記載の情報処理方法。

【請求項27】データを格納した情報記録媒体であり、複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した暗号化キーデータによって構成されるデータ部と、該データ部に格納される暗号化キーデータの前記階層ツリー構造における位置識別データとしてのタグ部とを含む有効化キーブロック（EKB）と、前記更新ノードキーによって暗号化したメッセージデータと、を格納したことを特徴とする情報記録媒体。

【請求項28】前記有効化キーブロック（EKB）に含まれる前記暗号化キーデータは、前記階層ツリー構造を構成するノードキーを下位ノードキーまたは下位リーフキーを用いて暗号化したデータであり、前記タグ部に格納される位置識別データは、前記有効化キーブロック（EKB）に格納された1以上の暗号化キーデータ各々のノード位置の下位の左右位置のノードまたはリーフ位置の暗号化キーデータの有無を示すタグとして構成されていることを特徴とする請求項27に記載の情報記録媒体。

【請求項29】前記有効化キーブロック（EKB）に含まれる前記暗号化キーデータは、該有効化キーブロック（EKB）を復号可能な末端ノードまたはリーフを最下段とした簡略化した2分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーのノードまたはリーフに対応するキーのみに基づいて構成され、前記タグ部に格納される位置識別データは、前記有効化キーブロック（EKB）のタグに対応する暗号化キーの格納の有無を示すデータを含む構成であることを特徴とする請求項27に記載の情報記録媒体。

【請求項30】複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号

6

化した有効化キーブロック（EKB）の生成処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

該有効化キーブロック（EKB）を復号可能な末端ノードまたはリーフを最下段とした簡略化した2分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築階層ツリーを生成するステップと、

前記再構築階層ツリーの構成ノードまたはリーフに対応するキーのみに基づいて有効化キーブロック（EKB）を生成するステップと、

前記有効化キーブロック（EKB）のタグに対応する暗号化キーの格納の有無を示すデータを前記タグ部に格納するステップと、

を含むことを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理システム、情報処理方法、および情報記録媒体、並びにプログラム提供媒体に関し、特に、暗号処理を伴うシステムにおける暗号処理鍵を配信するシステムおよび方法に関する。特に、木構造の階層的鍵配信方式を用い、さらに、階層的鍵配信ツリーを配信デバイスに応じて再構築して配信キーブロックに含まれるデータ量を削減することにより、配信メッセージ量を小さく抑えて、コンテンツキー配信、あるいは各種鍵の更新の際のデータ配信の負荷を軽減し、かつデータの安全性を保持することを可能とする情報処理システム、情報処理方法、および情報記録媒体、並びにプログラム提供媒体に関する。

【0002】

【従来の技術】昨今、ゲームプログラム、音声データ、画像データ等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）を、インターネット等のネットワーク、あるいはDVD、CD等の流通可能な記憶媒体を介しての流通が盛んになってきている。これらの流通コンテンツは、ユーザの所有するPC（Personal Computer）、ゲーム機器によってデータ受信、あるいは記憶媒体の装着がなされて再生されたり、あるいはPC等に付属する記録再生機器内の記録デバイス、例えばメモ리카ード、ハードディスク等に格納されて、格納媒体からの新たな再生により利用される。

【0003】ビデオゲーム機器、PC等の情報機器には、流通コンテンツをネットワークから受信するため、あるいはDVD、CD等にアクセスするためのインタフェースを有し、さらにコンテンツの再生に必要な制御手段、プログラム、データのメモリ領域として使用されるRAM、ROM等を有する。

【0004】音楽データ、画像データ、あるいはプログラム等の様々なコンテンツは、再生機器として利用されるゲーム機器、PC等の情報機器本体からのユーザ指

7

示、あるいは接続された入力手段を介したユーザの指示により記憶媒体から呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

【0005】ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウェアの使用を許諾し、許可のない複製等が行われないようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

【0006】ユーザに対する利用制限を実現する1つの手法が、配布コンテンツの暗号化処理である。すなわち、例えばインターネット等を介して暗号化された音声データ、画像データ、ゲームプログラム等の各種コンテンツを配布するとともに、正規ユーザであると確認された者に対してのみ、配布された暗号化コンテンツを復号する手段、すなわち復号鍵を付与する構成である。

【0007】暗号化データは、所定の手続きによる復号化処理によって利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

【0008】暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類があるが、その1つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にDES（データ暗号標準：Data encryption standard）がある。

【0009】上述の暗号化処理、復号化に用いられる暗号化鍵、復号化鍵は、例えばあるパスワード等に基づいてハッシュ関数等の一方向性関数を適用して得ることができる。一方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザが決めたパスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるパスワードを求めることは実質上不可能となる。

【0010】また、暗号化するとき使用する暗号化鍵による処理と、復号するとき使用する復号化鍵の処理とを異なるアルゴリズムとした方式がいわゆる公開鍵暗号化方式と呼ばれる方式である。公開鍵暗号化方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が発

8

行した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号処理が可能となる。秘密鍵は、公開鍵を発行した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号化方式の代表的なものにはRSA（Rivest-Shamir-Adleman）暗号がある。このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。

【0011】

【発明が解決しようとする課題】上記のようなコンテンツ配信システムでは、コンテンツを暗号化してユーザにネットワーク、あるいはDVD、CD等の記録媒体に格納して提供し、暗号化コンテンツを復号するコンテンツキーを正当なユーザにのみ提供する構成が多く採用されている。コンテンツキー自体の不正なコピー等を防ぐためのコンテンツキーを暗号化して正当なユーザに提供し、正当なユーザのみが有する復号キーを用いて暗号化コンテンツキーを復号してコンテンツキーを使用可能とする構成が提案されている。

【0012】正当なユーザであるか否かの判定は、一般には、例えばコンテンツの送信者であるコンテンツプロバイダとユーザデバイス間において、コンテンツ、あるいはコンテンツキーの配信前に認証処理を実行することによって行なう。一般的な認証処理においては、相手の確認を行なうとともに、その通信でのみ有効なセッションキーを生成して、認証が成立した場合に、生成したセッションキーを用いてデータ、例えばコンテンツあるいはコンテンツキーを暗号化して通信を行なう。認証方式には、共通鍵暗号方式を用いた相互認証と、公開鍵方式を使用した認証方式があるが、共通鍵を使った認証においては、システムワイドで共通鍵が必要になり、更新処理等の際に不便である。また、公開鍵方式においては、計算負荷が大きくまた必要なメモリ量も大きくなり、各デバイスにこのような処理手段を設けることは望ましい構成とはいえない。

【0013】本発明では、上述のようなデータの送信者、受信者間の相互認証処理に頼ることなく、正当なユーザに対してのみ、安全にデータを送信することを可能とするとともに、階層的鍵配信ツリーを配信デバイスに応じて再構築して配信キーブロックに含まれるデータ量を削減することにより、暗号化キーのデータ量を削減し、データ送信の負荷を軽減するとともに、各デバイスにおける暗号化キー取得のための処理の軽減を可能とした情報処理システム、情報処理方法、および情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

【0014】

【課題を解決するための手段】本発明の第1の側面は、

1 以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータを配信する情報処理システムであり、個々のデバイスは、複数の異なるデバイスをリーフとした階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するとともに、デバイスに対して配信される前記暗号化メッセージデータについての復号処理を前記キーセットを使用して実行する暗号処理手段を有し、前記デバイスに提供される暗号化メッセージデータは、前記階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した暗号化キーデータを含む有効化キープロック (EKB) の復号処理によって得られる更新ノードキーによって暗号化されたデータ構成であり、前記有効化キープロック (EKB) は、前記暗号化キーデータによって構成されるデータ部と、該データ部に格納される暗号化キーデータの階層ツリー構造における位置識別データとしてのタグ部とを含む構成であることを特徴とする情報処理システムにある。

【0015】さらに、本発明の情報処理システムの一実施態様において、前記有効化キープロック (EKB) に含まれる前記暗号化キーデータは、前記階層ツリー構造を構成するノードキーを下位ノードキーまたは下位リーフキーを用いて暗号化したデータであり、前記タグ部に格納される位置識別データは、前記有効化キープロック (EKB) に格納された1以上の暗号化キーデータ各々のノード位置の下位の左右ノードまたはリーフ位置の暗号化キーデータの有無を示すタグとして構成されていることを特徴とする。

【0016】さらに、本発明の情報処理システムの一実施態様において、前記有効化キープロック (EKB) に含まれる前記暗号化キーデータは、該有効化キープロック (EKB) を復号可能な末端ノードまたはリーフを最下段とした簡略化した2分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーのノードまたはリーフに対応するキーのみに基づいて構成され、前記タグ部に格納される位置識別データは、前記有効化キープロック (EKB) のタグに対応する暗号化キーの格納の有無を示すデータを含む構成であることを特徴とする。

【0017】さらに、本発明の情報処理システムの一実施態様において、前記有効化キープロック (EKB) に含まれる前記暗号化キーデータは、該有効化キープロック (EKB) を復号可能な末端ノードまたはリーフを最下段とした簡略化した2分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーのノードまたはリーフに対応するキー

のみに基づいて構成され、前記タグ部に格納される位置識別データは、前記有効化キープロック (EKB) に格納された1以上の暗号化キーデータ各々のノード位置の下位の左右ノードまたはリーフ位置の暗号化キーデータの有無を示すタグと、該タグに対応する暗号化キーの格納の有無を示すデータを含む構成であることを特徴とする。

【0018】さらに、本発明の情報処理システムの一実施態様において、前記再構築階層ツリーは、共通要素を持つデバイスの部分集合ツリーとして定義されるエンティティの頂点ノードであるサブルートを選択して構成されるツリーであることを特徴とする。

【0019】さらに、本発明の情報処理システムの一実施態様において、前記有効化キープロック (EKB) に含まれる前記暗号化キーデータは、該有効化キープロック (EKB) を復号可能な末端ノードまたはリーフを最下段とした簡略化した多分岐型ツリーにおいて、前記末端ノードまたはリーフと、該多分岐型ツリーの頂点とを直接接続するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーの頂点ノードおよび末端ノードまたはリーフに対応するキーのみに基づいて構成され、前記タグ部に格納される位置識別データは、前記有効化キープロック (EKB) のタグに対応する暗号化キーの格納の有無を示すデータを含む構成であることを特徴とする。

【0020】さらに、本発明の情報処理システムの一実施態様において、前記再構築階層ツリーは、簡略化した多分岐型ツリーを構成する頂点ノードと、簡略化したツリーを構成する末端ノードまたはリーフとを直接、接続した3以上の分岐を持つツリーであることを特徴とする。

【0021】さらに、本発明の情報処理システムの一実施態様において、前記デバイスにおける前記暗号処理手段は、前記有効化キープロック (EKB) の前記タグ部のデータにより、前記暗号化キーデータを順次抽出して、復号処理を実行し、前記更新ノードキーを取得し、該取得した更新ノードキーにより前記暗号化メッセージデータの復号を実行する構成であることを特徴とする。

【0022】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーであることを特徴とする。

【0023】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする。

【0024】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータは、コンテンツのインテグリティ・チェック値 (ICV) 生成キーであることを特徴とする。

【0025】さらに、本発明の情報処理システムの一実

施態様において、前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする。

【0026】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータは、プログラムコードであることを特徴とする。

【0027】さらに、本発明の第2の側面は、1以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータを配信する情報処理方法であり、複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した暗号化キーデータを含むデータ部と、該データ部に格納される暗号化キーデータの前記階層ツリー構造における位置識別データとしてのタグ部とを含む有効化キーブロック（EKB）を生成する有効化キーブロック（EKB）生成ステップと、前記更新ノードキーによって暗号化したメッセージデータを生成してデバイスに対して配信するメッセージデータ配信ステップと、を有することを特徴とする情報処理方法にある。

【0028】さらに、本発明の情報処理方法の一実施態様において、前記階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するデバイスにおいて、前記暗号化メッセージデータについての復号処理を前記キーセットを使用して実行する復号処理ステップを有することを特徴とする。

【0029】さらに、本発明の情報処理方法の一実施態様において、前記有効化キーブロック（EKB）生成ステップは、前記階層ツリー構造を構成するノードキーを下位ノードキーまたは下位リーフキーを用いて暗号化して前記暗号化キーデータを生成するステップと、前記有効化キーブロック（EKB）に格納される1以上の暗号化キーデータ各々のノード位置の下位の左右位置のノードまたはリーフ位置の暗号化キーデータの有無を示すタグを生成して前記タグ部に格納するステップとを含むことを特徴とする。

【0030】さらに、本発明の情報処理方法の一実施態様において、前記有効化キーブロック（EKB）生成ステップは、該有効化キーブロック（EKB）を復号可能な末端ノードまたはリーフを最下段とした簡略化した2分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築階層ツリーを生成するステップと、前記再構築階層ツリーの構成ノードまたはリーフに対応するキーのみに基づいて有効化キーブロック（EKB）を生成するステップと、前記有効化キーブロック

（EKB）のタグに対応する暗号化キーの格納の有無を示すデータを前記タグ部に格納するステップと、を含む

ことを特徴とする。

【0031】さらに、本発明の情報処理方法の一実施態様において、前記再構築階層ツリーを生成するステップは、共通要素を持つデバイスの部分集合ツリーとして定義されるエンティティの頂点ノードであるサブルートを選択して実行されるツリー生成処理であることを特徴とする。

【0032】さらに、本発明の情報処理方法の一実施態様において、前記有効化キーブロック（EKB）生成ステップは、該有効化キーブロック（EKB）を復号可能な末端ノードまたはリーフを最下段とした簡略化した多分岐型ツリーにおいて、前記末端ノードまたはリーフと、該多分岐型ツリーの頂点とを直接接続するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーを生成するステップと、前記有効化キーブロック（EKB）のタグに対応する暗号化キーの格納の有無を示すデータを前記タグ部に格納するステップと、を含むことを特徴とする。

【0033】さらに、本発明の情報処理方法の一実施態様において、前記再構築階層ツリーの生成ステップにおいて生成する再構築階層ツリーは、簡略化した多分岐型ツリーを構成する頂点ノードと、簡略化したツリーを構成する末端ノードまたはリーフとを直接、接続した3以上の分岐を持つツリーとして生成することを特徴とする。

【0034】さらに、本発明の情報処理方法の一実施態様において、前記復号処理ステップは、前記有効化キーブロック（EKB）の前記タグ部に格納された位置識別データに基づいて前記データ部に格納された暗号化キーデータを順次抽出して順次復号処理を実行することにより前記更新ノードキーを取得する更新ノードキー取得ステップと、前記更新ノードキーにより前記暗号化メッセージデータの復号を実行するメッセージデータ復号ステップとを含むことを特徴とする。

【0035】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーであることを特徴とする。

【0036】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする。

【0037】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータは、コンテンツのインテグリティ・チェック値（ICV）生成キーであることを特徴とする。

【0038】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする。

【0039】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータは、プログラムコー

13

ドであることを特徴とする。

【0040】さらに、本発明の第3の側面は、データを格納した情報記録媒体であり、複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した暗号化キーデータによって構成されるデータ部と、該データ部に格納される暗号化キーデータの前記階層ツリー構造における位置識別データとしてのタグ部とを含む有効化キープロック（EKB）と、前記更新ノードキーによって暗号化したメッセージデータと、を格納したことを特徴とする情報記録媒体にある。

【0041】さらに、本発明の情報記録媒体の一実施態様において、前記有効化キープロック（EKB）に含まれる前記暗号化キーデータは、前記階層ツリー構造を構成するノードキーを下位ノードキーまたは下位リーフキーを用いて暗号化したデータであり、前記タグ部に格納される位置識別データは、前記有効化キープロック（EKB）に格納された1以上の暗号化キーデータ各々のノード位置の下位の左右位置のノードまたはリーフ位置の暗号化キーデータの有無を示すタグとして構成されていることを特徴とする。

【0042】さらに、本発明の情報記録媒体の一実施態様において、前記有効化キープロック（EKB）に含まれる前記暗号化キーデータは、該有効化キープロック

（EKB）を復号可能な末端ノードまたはリーフを最下段とした簡略化した2分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーのノードまたはリーフに対応するキーのみに基づいて構成され、前記タグ部に格納される位置識別データは、前記有効化キープロック（EKB）のタグに対応する暗号化キーの格納の有無を示すデータを含む構成であることを特徴とする。

【0043】さらに、本発明の第4の側面は、複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キープロック（EKB）の生成処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、該有効化キープロック（EKB）を復号可能な末端ノードまたはリーフを最下段とした簡略化した2分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築階層ツリーを生成するステップと、

14

前記再構築階層ツリーの構成ノードまたはリーフに対応するキーのみに基づいて有効化キープロック（EKB）を生成するステップと、前記有効化キープロック（EKB）のタグに対応する暗号化キーの格納の有無を示すデータを前記タグ部に格納するステップと、を含むことを特徴とするプログラム提供媒体にある。

【0044】

【作用】本発明の構成においては、ツリー（木）構造の階層的構造の暗号化鍵配信構成を用いることにより、キー更新に必要な配信メッセージ量を小さく抑えている。すなわち、各機器をn分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、例えばコンテンツデータの暗号鍵であるコンテンツキーもしくは認証処理に用いる認証キー、あるいはプログラムコード等を有効化キープロックとともに配信する構成としている。

【0045】さらに、有効化キープロックを暗号化キーデータ部と、暗号化キーの位置を示すタグ部によって構成し、データ量を少なくし、デバイスにおける復号処理を用意かつ迅速に実行することを可能としている。本構成により、正当なデバイスのみが復号可能なデータを安全に配信することが可能となる。

【0046】なお、本発明の第4の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【0047】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【0048】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0049】

【発明の実施の形態】〔システム概要〕図1に本発明のデータ処理システムが適用可能なコンテンツ配信システム例を示す。コンテンツの配信側10は、コンテンツ受信側20の有する様々なコンテンツ再生可能な機器に対してコンテンツ、あるいはコンテンツキーを暗号化して送信する。受信側20における機器では、受信した暗号化コンテンツ、あるいは暗号化コンテンツキー等を復号してコンテンツあるいはコンテンツキーを取得して、画

15

像データ、音声データの再生、あるいは各種プログラムの実行等を行なう。コンテンツの配信側10とコンテンツ受信側20との間のデータ交換は、インターネット等のネットワークを介して、あるいはDVD、CD等の流通可能な記憶媒体を介して実行される。

【0050】コンテンツの配信側10のデータ配信手段としては、インターネット11、衛星放送12、電話回線13、DVD、CD等のメディア14等があり、一方、コンテンツ受信側20のデバイスとしては、パーソナルコンピュータ(PC)21、ポータブルデバイス(PD)22、携帯電話、PDA(Personal Digital Assistants)等の携帯機器23、DVD、CDプレーヤ等の記録再生器24、ゲーム端末等の再生専用器25等がある。これらコンテンツ受信側20の各デバイスは、コンテンツ配信側10から提供されたコンテンツをネットワーク等の通信手段あるいは、あるいはメディア30から取得する。

【0051】[デバイス構成]図2に、図1に示すコンテンツ受信側20のデバイスの一例として、記録再生装置100の構成ブロック図を示す。記録再生装置100は、入出力I/F(Interface)120、MPEG(Moving Picture Experts Group)コーデック130、A/D、D/Aコンバータ141を備えた入出力I/F(Interface)140、暗号処理手段150、ROM(Read Only Memory)160、CPU(Central Processing Unit)170、メモリ180、記録媒体195のドライブ190を有し、これらはバス110によって相互に接続されている。

【0052】入出力I/F120は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス110上に出力するとともに、バス110上のデジタル信号を受信し、外部に出力する。MPEGコーデック130は、バス110を介して供給されるMPEG符号化されたデータを、MPEGデコードし、入出力I/F140に出力するとともに、入出力I/F140から供給されるデジタル信号をMPEGエンコードしてバス110上に出力する。入出力I/F140は、A/D、D/Aコンバータ141を内蔵している。入出力I/F140は、外部から供給されるコンテンツとしてのアナログ信号を受信し、A/D、D/Aコンバータ141でA/D(Analog Digital)変換することで、デジタル信号として、MPEGコーデック130に出力するとともに、MPEGコーデック130からのデジタル信号を、A/D、D/Aコンバータ141でD/A(Digital Analog)変換することで、アナログ信号として、外部に出力する。

【0053】暗号処理手段150は、例えば、1チップのLSI(Large Scale Integrated Circuit)で構成され、バス110を介して供給されるコンテンツとしてのデジタル信号の暗号化、復号処理、あるいは認証処理

16

を実行し、暗号データ、復号データ等をバス110上に出力する構成を持つ。なお、暗号処理手段150は1チップLSIに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

【0054】ROM160は、記録再生装置によって処理されるプログラムデータを格納する。CPU170は、ROM160、メモリ180に記憶されたプログラムを実行することで、MPEGコーデック130や暗号処理手段150等を制御する。メモリ180は、例えば、不揮発性メモリで、CPU170が実行するプログラムや、CPU170の動作上必要なデータ、さらにデバイスによって実行される暗号処理に使用されるキーセットを記憶する。キーセットについては後段で説明する。ドライブ190は、デジタルデータを記録再生可能な記録媒体195を駆動することにより、記録媒体195からデジタルデータを読み出し(再生し)、バス110上に出力するとともに、バス110を介して供給されるデジタルデータを、記録媒体195に供給して記録させる。

【0055】記録媒体195は、例えば、DVD、CD等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはRAM等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、本実施の形態では、ドライブ190に対して着脱可能な構成であるとする。但し、記録媒体195は、記録再生装置100に内蔵する構成としてもよい。

【0056】なお、図2に示す暗号処理手段150は、1つのワンチップLSIとして構成してもよく、また、ソフトウェア、ハードウェアを組み合わせた構成によって実現する構成としてもよい。

【0057】[キー配信構成としてのツリー(木)構造について]次に、図1に示すコンテンツ配信側10からコンテンツ受信側20の各デバイスに暗号データを配信する場合における各デバイスにおける暗号処理鍵の保有構成およびデータ配信構成を図3を用いて説明する。

【0058】図3の最下段に示すナンバ0~15がコンテンツ受信側20の個々のデバイスである。すなわち図3に示す階層ツリー(木)構造の各葉(リーフ:leaf)がそれぞれのデバイスに相当する。

【0059】各デバイス0~15は、製造時あるいは出荷時、あるいはその後において、図3に示す階層ツリー(木)構造における、自分のリーフからルートに至るまでのノードに割り当てられた鍵(ノードキー)および各リーフのリーフキーからなるキーセットをメモリに格納する。図3の最下段に示すK0000~K1111が各デバイス0~15にそれぞれ割り当てられたリーフキーであり、最上段のKR(ルートキー)から、最下段から2番目の節(ノード)に記載されたキー:KR~K11

17

1をノードキーとする。

【0060】図3に示すツリー構成において、例えばデバイス0はリーフキーK0000と、ノードキー：K000、K00、K0、KRを所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。なお、図3のツリーにはデバイスが0～15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【0061】また、図3のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたDVD、CD、MD、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図3に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

【0062】これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図3の点線で囲んだ部分、すなわちデバイス0、1、2、3を同一の記録媒体を用いる1つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、各デバイス共通に使用するコンテンツキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図3の点線で囲んだ部分、すなわちデバイス0、1、2、3を1つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図3のツリー中に複数存在する。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、メッセージデータ配信手段として機能する。

【0063】なお、ノードキー、リーフキーは、ある1つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

【0064】このツリー構造において、図3から明らかのように、1つのグループに含まれる3つのデバイス0、1、2、3はノードキーとして共通のキーK00、

18

K0、KRを保有する。このノードキー共有構成を利用することにより、例えば共通のコンテンツキーをデバイス0、1、2、3のみに提供することが可能となる。たとえば、共通に保有するノードキーK00自体をコンテンツキーとして設定すれば、新たな鍵送付を実行することなくデバイス0、1、2、3のみが共通のコンテンツキーの設定が可能である。また、新たなコンテンツキーKconをノードキーK00で暗号化した値Enc(K00, Kcon)を、ネットワークを介してあるいは記録媒体に格納してデバイス0、1、2、3に配布すれば、デバイス0、1、2、3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc(K00, Kcon)を解いてコンテンツキー：Kconを得ることが可能となる。なお、Enc(Ka, Kb)はKbをKaによって暗号化したデータであることを示す。

【0065】また、ある時点tにおいて、デバイス3の所有する鍵：K0011、K001、K00、K0、KRが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス0、1、2、3のグループ）で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキー：K001、K00、K0、KRをそれぞれ新たな鍵K(t)001、K(t)00、K(t)0、K(t)Rに更新し、デバイス0、1、2にその更新キーを伝える必要がある。ここで、K(t)aaaは、鍵Kaaaの世代（Generation）：tの更新キーであることを示す。

【0066】更新キーの配布処理について説明する。キーの更新は、例えば、図4（A）に示す有効化キーブロック（EKB：Enabling Key Block）と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス0、1、2に供給することによって実行される。なお、有効化キーブロック（EKB）は、図3に示すようなツリー構造を構成する各リーフに対応するデバイスに新たに更新されたキーを配布するための暗号化キーによって構成される。有効化キーブロック（EKB）は、キー更新ブロック（KRB：KeyRenewal Block）と呼ばれることもある。

【0067】図4（A）に示す有効化キーブロック（EKB）には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図4の例は、図3に示すツリー構造中のデバイス0、1、2において、世代tの更新ノードキーを配布することを目的として形成されたブロックデータである。図3から明らかなように、デバイス0、デバイス1は、更新ノードキーとしてK(t)00、K(t)0、K(t)Rが必要であり、デバイス2は、更新ノードキーとしてK(t)001、K(t)00、K(t)0、

19

K(t) Rが必要である。

【0068】図4(A)のEKBに示されるようにEKBには複数の暗号化キーが含まれる。最下段の暗号化キーは、Enc(K0010, K(t)001)である。これはデバイス2の持つリーフキーK0010によって暗号化された更新ノードキーK(t)001であり、デバイス2は、自身の持つリーフキーによってこの暗号化キーを復号し、K(t)001を得ることができる。また、復号により得たK(t)001を用いて、図4

(A)の下から2段目の暗号化キーEnc(K(t)001, K(t)00)を復号可能となり、更新ノードキーK(t)00を得ることができる。以下順次、図4

(A)の上から2段目の暗号化キーEnc(K(t)00, K(t)0)を復号し、更新ノードキーK(t)0、図4(A)の上から1段目の暗号化キーEnc(K(t)0, K(t)R)を復号しK(t)Rを得る。一方、デバイスK0000、K0001は、ノードキーK000は更新する対象に含まれておらず、更新ノードキーとして必要なのは、K(t)00、K(t)0、K(t)Rである。デバイスK0000、K0001は、

図4(A)の上から3段目の暗号化キーEnc(K000, K(t)00)を復号しK(t)00、を取得し、以下、図4(A)の上から2段目の暗号化キーEnc

(K(t)00, K(t)0)を復号し、更新ノードキーK(t)0、図4(A)の上から1段目の暗号化キーEnc(K(t)0, K(t)R)を復号しK(t)Rを得る。このようにして、デバイス0、1、2は更新した鍵K(t)Rを得ることができる。なお、図4(A)のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【0069】図3に示すツリー構造の上位段のノードキー：K(t)0、K(t)Rの更新が不要であり、ノードキーK00のみの更新処理が必要である場合には、図4(B)の有効化キーブロック(EKB)を用いることで、更新ノードキーK(t)00をデバイス0、1、2に配布することができる。

【0070】図4(B)に示すEKBは、例えば特定のグループにおいて共有する新たなコンテンツキーを配布する場合に利用可能である。具体例として、図3に点線で示すグループ内のデバイス0、1、2、3がある記録媒体を用いており、新たな共通のコンテンツキーK

(t)conが必要であるとする。このとき、デバイス0、1、2、3の共通のノードキーK00を更新したK(t)00を用いて新たな共通の更新コンテンツキー：K(t)conを暗号化したデータEnc(K(t), K(t)con)を図4(B)に示すEKBとともに配布する。この配布により、デバイス4など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

【0071】すなわち、デバイス0、1、2はEKBを

20

処理して得たK(t)00を用いて上記暗号文を復号すれば、t時点でのコンテンツキーK(t)conを得ることが可能になる。

【0072】[EKBを使用したコンテンツキーの配布]図5に、t時点でのコンテンツキーK(t)conを得る処理例として、K(t)00を用いて新たな共通のコンテンツキーK(t)conを暗号化したデータEnc(K(t)00, K(t)con)と図4(B)に示すEKBとを記録媒体を介して受領したデバイス0の処理を示す。すなわちEKBによる暗号化メッセージデータをコンテンツキーK(t)conとした例である。

【0073】図5に示すように、デバイス0は、記録媒体に格納されている世代：t時点のEKBと自分があらかじめ格納しているノードキーK000を用いて上述したと同様のEKB処理により、ノードキーK(t)00を生成する。さらに、復号した更新ノードキーK(t)00を用いて更新コンテンツキーK(t)conを復号して、後にそれを使用するために自分だけが持つリーフキーK0000で暗号化して格納する。

【0074】[EKBのフォーマット]図6に有効化キーブロック(EKB)のフォーマット例を示す。バージョン601は、有効化キーブロック(EKB)のバージョンを示す識別子である。なお、バージョンは最新のEKBを識別する機能とコンテンツとの対応関係を示す機能を持つ。デプスは、有効化キーブロック(EKB)の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ603は、有効化キーブロック(EKB)中のデータ部の位置を示すポインタであり、タグポインタ604はタグ部の位置、署名ポインタ605は署名の位置を示すポインタである。

【0075】データ部606は、例えば更新するノードキーを暗号化したデータを格納する。例えば図5に示すような更新されたノードキーに関する各暗号化キー等を格納する。

【0076】タグ部607は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図7を用いて説明する。図7では、データとして先に図4(A)で説明した有効化キーブロック(EKB)を送付する例を示している。この時のデータは、図7の表(b)に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キーK(t)Rが含まれているので、トップノードアドレスはKRとなる。このとき、例えば最上段のデータEnc(K(t)0, K(t)R)は、図7の(a)に示す階層ツリーに示す位置にある。ここで、次のデータは、Enc(K(t)00, K(t)0)であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが0、ない場合は1が設定される。タグは{左(L)タグ、右(R)タグ}とし

21

て設定される。最上段のデータEnc (K (t) 0, K (t) R) の左にはデータがあるので、Lタグ=0、右にはデータがないので、Rタグ=1となる。以下、すべてのデータにタグが設定され、図7 (c) に示すデータ列、およびタグ列が構成される。

【0077】タグは、データEnc (Kxxx, Kyyy) がツリー構造のどこに位置しているのかを示すために設定されるものである。データ部に格納されるキーデータEnc (Kxxx, Kyyy) . . . は、単純に暗号化されたキーの羅列データに過ぎないので、上述したタグによってデータとして格納された暗号化キーのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図4で説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、

0 : Enc (K (t) 0, K (t) root)
00 : Enc (K (t) 00, K (t) 0)
000 : Enc (K (t) 000, K (T) 00)

. . . のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

【0078】図6に戻って、EKBフォーマットについてさらに説明する。署名 (Signature) は、有効化キーブロック (EKB) を発行した例えば鍵管理センタ、コンテンツロバイダ、決済機関等が実行する電子署名である。EKBを受領したデバイスは署名検証によって正当な有効化キーブロック (EKB) 発行者が発行した有効化キーブロック (EKB) であることを確認する。

【0079】[EKBを使用したコンテンツキーおよびコンテンツの配信] 上述の例では、コンテンツキーのみをEKBとともに送付する例について説明したが、コンテンツキーで暗号化したコンテンツと、コンテンツキー暗号キーで暗号化したコンテンツキーと、EKBによって暗号化したコンテンツキー暗号鍵を併せて送付する構成について以下説明する。

【0080】図8にこのデータ構成を示す。図8 (a) に示す構成において、Enc (Kcon, content) 801は、コンテンツ (Content) をコンテンツキー (Kcon) で暗号化したデータであり、Enc (KEK, Kcon) 802は、コンテンツキー (Kcon) をコンテンツキー暗号キー (KEK : Key Encryption Key) で暗号化したデータであり、Enc (EKB, KEK) 803は、コンテンツキー暗号キーKEKを有効化キーブロック (EKB) によって暗号化したデータであることを示す。

【0081】ここで、コンテンツキー暗号キーKEKは、図3で示すノードキー (K000, K00...)、あ

22

るいはルートキー (KR) 自体であってもよく、またノードキー (K000, K00...)、あるいはルートキー (KR) によって暗号化されたキーであってもよい。

【0082】図8 (b) は、複数のコンテンツがメディアに記録され、それぞれが同じEnc (EKB, KEK) 805を利用している場合の構成例を示す、このような構成においては、各データに同じEnc (EKB, KEK) を付加することなく、Enc (EKB, KEK) にリンクするリンク先を示すデータを各データに付加する構成とすることができる。

【0083】図9にコンテンツキー暗号キーKEKを、図3に示すノードキーK00を更新した更新ノードキーK (t) 00として構成した場合の例を示す。この場合、図3の点線枠で囲んだグループにおいてデバイス3が、例えば鍵の漏洩によりリボーク (排除) されているとして、他のグループのメンバ、すなわち、デバイス0, 1, 2に対して図9に示す (a) 有効化キーブロック (EKB) と、 (b) コンテンツキー (Kcon) をコンテンツキー暗号キー (KEK=K (t) 00) で暗号化したデータと、 (c) コンテンツ (content) をコンテンツキー (Kcon) で暗号化したデータとを配信することにより、デバイス0, 1, 2はコンテンツを得ることができる。

【0084】図9の右側には、デバイス0における復号手順を示してある。デバイス0は、まず、受領した有効化キーブロックから自身の保有するリーフキーK000を用いた復号処理により、コンテンツキー暗号キー (KEK=K (t) 00) を取得する。次に、K (t) 00による復号によりコンテンツキーKconを取得し、さらにコンテンツキーKconによりコンテンツの復号を行なう。これらの処理により、デバイス0はコンテンツを利用可能となる。デバイス1, 2においても各々異なる処理手順でEKBを処理することにより、コンテンツキー暗号キー (KEK=K (t) 00) を取得することが可能となり、同様にコンテンツを利用することが可能となる。

【0085】図3に示す他のグループのデバイス4, 5, 6...は、この同様のデータ (EKB) を受信したとしても、自身の保有するリーフキー、ノードキーを用いてコンテンツキー暗号キー (KEK=K (t) 00) を取得することができない。同様にリボークされたデバイス3においても、自身の保有するリーフキー、ノードキーでは、コンテンツキー暗号キー (KEK=K (t) 00) を取得することができず、正当な権利を有するデバイスのみがコンテンツを復号して利用することが可能となる。

【0086】このように、EKBを利用したコンテンツキーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能とした暗号化コンテンツを配信することが可能となる。

23

【0087】なお、有効化キープブロック（EKB）、コンテンツキー、暗号化コンテンツ等は、ネットワークを介して安全に配信することが可能な構成であるが、有効化キープブロック（EKB）、コンテンツキー、暗号化コンテンツをDVD、CD等の記録媒体に格納してユーザに提供することも可能である。この場合、記録媒体に格納された暗号化コンテンツの復号には、同一の記録媒体に格納された有効化キープブロック（EKB）の復号により得られるコンテンツキーを使用するように構成すれば、予め正当権利者のみが保有するリーフキー、ノードキーによってのみ利用可能な暗号化コンテンツの配布処理、すなわち利用可能なユーザデバイスを限定したコンテンツ配布が簡易な構成で実現可能となる。

【0088】図10に記録媒体に暗号化コンテンツとともに有効化キープブロック（EKB）を格納した構成例を示す。図10に示す例においては、記録媒体にコンテンツC1～C4が格納され、さらに各格納コンテンツに対応する有効化キープブロック（EKB）を対応付けたデータが格納され、さらにバージョンMの有効化キープブロック（EKB_M）が格納されている。例えばEKB_1はコンテンツC1を暗号化したコンテンツキーKcon1を生成するのに使用され、例えばEKB_2はコンテンツC2を暗号化したコンテンツキーKcon2を生成するのに使用される。この例では、バージョンMの有効化キープブロック（EKB_M）が記録媒体に格納されており、コンテンツC3、C4は有効化キープブロック（EKB_M）に対応付けられているので、有効化キープブロック（EKB_M）の復号によりコンテンツC3、C4のコンテンツキーを取得することができる。EKB_1、EKB_2はディスクに格納されていないので、新たな提供手段、例えばネットワーク配信、あるいは記録媒体による配信によってそれぞれのコンテンツキーを復号するために必要なEKB_1、EKB_2を取得することが必要となる。

【0089】図11に、複数のデバイス間でコンテンツキーが流通する場合のEKBを利用したコンテンツキーの配信と、従来のコンテンツキー配信処理の比較例を示す。上段（a）が従来構成であり、下段（b）が本発明の有効化キープブロック（EKB）を利用した例である。なお、図11においてKa（Kb）は、KbをKaで暗号化したデータであることを示す。

【0090】（a）に示すように、従来は、データ送受信者の正当性を確認し、またデータ送信の暗号化処理に使用するセッションキーKsesを共有するために各デバイス間において、認証処理および鍵交換処理（AKE: Authentication and Key Exchange）を実行し、認証が成立したことを条件としてセッションキーKsesでコンテンツキーKconを暗号化して送信する処理を行っていた。

【0091】例えば図11（a）のPCにおいては、受

24

信したセッションキーで暗号化したコンテンツキーKses（Kcon）をセッションキーで復号してKconを得ることが可能であり、さらに取得したKconをPC自体の保有する保存キーKstrで暗号化して自身のメモリに保存することが可能となる。

【0092】図11（a）において、コンテンツプロバイダは、図11（a）の記録デバイス1101にのみデータを利用可能な形で配信したい場合でも、間にPC、再生装置が存在する場合は、図11（a）に示すように認証処理を実行し、それぞれのセッションキーでコンテンツキーを暗号化して配信するといった処理が必要となる。また、間に介在するPC、再生装置においても認証処理において生成し共有することになったセッションキーを用いることで暗号化コンテンツキーを復号してコンテンツキーを取得可能となる。

【0093】一方、図11（b）の下段に示す有効化キープブロック（EKB）を利用した例においては、コンテンツプロバイダから有効化キープブロック（EKB）と、有効化キープブロック（EKB）の処理によって得られるノードキー、またはルートキーによってコンテンツキーKconを暗号化したデータ（図の例ではKroot（Kcon））を配信することにより、配信したEKBの処理が可能な機器においてのみコンテンツキーKconを復号して取得することが可能になる。

【0094】従って、例えば図11（b）の右端にのみ利用可能な有効化キープブロック（EKB）を生成して、その有効化キープブロック（EKB）と、そのEKB処理によって得られるノードキー、またはルートキーによってコンテンツキーKconを暗号化したデータを併せて送ることにより、間に存在するPC、再生機器等は、自身の有するリーフキー、ノードキーによっては、EKBの処理を実行することができない。従って、データ送受信デバイス間での認証処理、セッションキーの生成、セッションキーによるコンテンツキーKconの暗号化処理といった処理を実行することなく、安全に正当なデバイスに対してのみ利用可能なコンテンツキーを配信することが可能となる。

【0095】PC、記録再生器にも利用可能なコンテンツキーを配信したい場合は、それぞれにおいて処理可能な有効化キープブロック（EKB）を生成して、配信することにより、共通のコンテンツキーを取得することが可能となる。

【0096】〔有効化キープブロック（EKB）を使用した認証キーの配信（共通鍵方式）〕上述の有効化キープブロック（EKB）を使用したデータあるいはキーの配信において、デバイス間で転送される有効化キープブロック（EKB）およびコンテンツあるいはコンテンツキーは常に同じ暗号化形態を維持しているため、データ伝走路を盗み出して記録し、再度、後で転送する、いわゆるリプレイアタックにより、不正コピーが生成される可能性

25

がある。これを防ぐ構成としては、データ転送デバイス間において、従来と同様の認証処理および鍵交換処理を実行することが有効な手段である。ここでは、この認証処理および鍵交換処理を実行する際に使用する認証キー K_{ake} を上述の有効化キープブロック (EKB) を使用してデバイスに配信することにより、安全な秘密鍵として共有する認証キーを持ち、共通鍵方式に従った認証処理を実行する構成について説明する。すなわち EKB による暗号化メッセージデータを認証キーとした例である。

【0097】図12に、共通鍵暗号方式を用いた相互認証方法 (ISO/IEC 9798-2) を示す。図12においては、共通鍵暗号方式として DES を用いているが、共通鍵暗号方式であれば他の方式も可能である。図12において、まず、Bが64ビットの乱数 R_b を生成し、 R_b および自己の ID である ID (b) を A に送信する。これを受信した A は、新たに64ビットの乱数 R_a を生成し、 R_a 、 R_b 、ID (b) の順に、DES の CBC モードで鍵 K_{ab} を用いてデータを暗号化し、B に返送する。なお、鍵 K_{ab} は、A および B に共通の秘密鍵としてそれぞれの記録素子内に格納する鍵である。DES の CBC モードを用いた鍵 K_{ab} による暗号化処理は、例えば DES を用いた処理においては、初期値と R_a とを排他的論理和し、DES 暗号化部において、鍵 K_{ab} を用いて暗号化し、暗号文 E_1 を生成し、続けて暗号文 E_1 と R_b とを排他的論理和し、DES 暗号化部において、鍵 K_{ab} を用いて暗号化し、暗号文 E_2 を生成し、さらに、暗号文 E_2 と ID (b) とを排他的論理和し、DES 暗号化部において、鍵 K_{ab} を用いて暗号化して生成した暗号文 E_3 とによって送信データ (Token-AB) を生成する。

【0098】これを受信した B は、受信データを、やはり共通の秘密鍵としてそれぞれの記録素子内に格納する鍵 K_{ab} (認証キー) で復号化する。受信データの復号化方法は、まず、暗号文 E_1 を認証キー K_{ab} で復号化し、乱数 R_a を得る。次に、暗号文 E_2 を認証キー K_{ab} で復号化し、その結果と E_1 を排他的論理和し、 R_b を得る。最後に、暗号文 E_3 を認証キー K_{ab} で復号化し、その結果と E_2 を排他的論理和し、ID (b) を得る。こうして得られた R_a 、 R_b 、ID (b) のうち、 R_b および ID (b) が、B が送信したものと一致するか検証する。この検証に通った場合、B は A を正当なものとして認証する。

【0099】次に B は、認証後に使用するセッションキー (K_{ses}) を生成する (生成方法は、乱数を用いる)。そして、 R_b 、 R_a 、 K_{ses} の順に、DES の CBC モードで認証キー K_{ab} を用いて暗号化し、A に返送する。

【0100】これを受信した A は、受信データを認証キー K_{ab} で復号化する。受信データの復号化方法は、B

26

の復号化処理と同様であるので、ここでは詳細を省略する。こうして得られた R_b 、 R_a 、 K_{ses} の内、 R_b および R_a が、A が送信したものと一致するか検証する。この検証に通った場合、A は B を正当なものとして認証する。互いに相手を認証した後は、セッションキー K_{ses} は、認証後の秘密通信のための共通鍵として利用される。

【0101】なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものと

10

して処理を中断する。

【0102】上述の認証処理においては、A、B は共通の認証キー K_{ab} を共有する。この共通鍵 K_{ab} を上述の有効化キープブロック (EKB) を使用してデバイスに配信する。

【0103】例えば、図12の例では、A、または B のいずれかが他方が復号可能な有効化キープブロック (EKB) を生成して生成した有効化キープブロック (EKB) によって認証キー K_{ab} を暗号化して、他方に送信する構成としてもよいし、あるいは第3者がデバイス A、B に対して双方が利用可能な有効化キープブロック (EKB) を生成してデバイス A、B に対して生成した有効化キープブロック (EKB) によって認証キー K_{ab} を暗号化して配信する構成としてもよい。

20

【0104】図13および図14に複数のデバイスに共通の認証キー K_{ake} を有効化キープブロック (EKB) によって配信する構成例を示す。図13はデバイス 0、1、2、3 に対して復号可能な認証キー K_{ake} を配信する例、図14はデバイス 0、1、2、3 中のデバイス 3 をリポーク (排除) してデバイス 0、1、2 に対してのみ復号可能な認証キーを配信する例を示す。

30

【0105】図13の例では、更新ノードキー $K(t)00$ によって、認証キー K_{ake} を暗号化したデータ (b) とともに、デバイス 0、1、2、3 においてそれぞれの有するノードキー、リーフキーを用いて更新されたノードキー $K(t)00$ を復号可能な有効化キープブロック (EKB) を生成して配信する。それぞれのデバイスは、図13の右側に示すようにまず、EKB を処理 (復号) することにより、更新されたノードキー $K(t)00$ を取得し、次に、取得したノードキー $K(t)00$ を用いて暗号化された認証キー: $Enc(K(t)00, K_{ake})$ を復号して認証キー K_{ake} を得ることが可能となる。

40

【0106】その他のデバイス 4、5、6、7... は同一の有効化キープブロック (EKB) を受信しても自身の保有するノードキー、リーフキーでは、EKB を処理して更新されたノードキー $K(t)00$ を取得することができないので、安全に正当なデバイスに対してのみ認証キーを送付することができる。

【0107】一方、図14の例は、図3の点線枠で囲んだグループにおいてデバイス 3 が、例えば鍵の漏洩によ

50

りリボーク（排除）されているとして、他のグループのメンバ、すなわち、デバイス0, 1, 2, に対してのみ復号可能な有効化キープブロック（EKB）を生成して配信した例である。図14に示す（a）有効化キープブロック（EKB）と、（b）認証キー（Kake）をノードキー（K(t)00）で暗号化したデータを配信する。

【0108】図14の右側には、復号手順を示してある。デバイス0, 1, 2は、まず、受領した有効化キープブロックから自身の保有するリーフキーまたはノードキーを用いた復号処理により、更新ノードキー（K(t)00）を取得する。次に、K(t)00による復号により認証キーKakeを取得する。

【0109】図3に示す他のグループのデバイス4, 5, 6…は、この同様のデータ（EKB）を受信したとしても、自身の保有するリーフキー、ノードキーを用いて更新ノードキー（K(t)00）を取得することができない。同様にリボークされたデバイス3においても、自身の保有するリーフキー、ノードキーでは、更新ノードキー（K(t)00）を取得することができず、正当な権利を有するデバイスのみが認証キーを復号して利用することが可能となる。

【0110】このように、EKBを利用した認証キーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能とした認証キーを配信することが可能となる。

【0111】〔公開鍵認証と有効化キープブロック（EKB）を使用したコンテンツキーの配信〕次に、公開鍵認証と有効化キープブロック（EKB）を使用したコンテンツキーの配信処理について説明する。まず、公開鍵暗号方式である160ビット長の楕円曲線暗号を用いた相互認証方法を、図15を用いて説明する。図15において、公開鍵暗号方式としてECCを用いているが、同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも160ビットでなくてもよい。図15において、まずBが、64ビットの乱数Rbを生成し、Aに送信する。これを受信したAは、新たに64ビットの乱数Raおよび素数pより小さい乱数Akを生成する。そして、ベースポイントGをAk倍した点Av=Ak×Gを求め、Ra、Rb、Av（X座標とY座標）に対する電子署名A.Sigを生成し、Aの公開鍵証明書とともにBに返送する。ここで、RaおよびRbはそれぞれ64ビット、AvのX座標とY座標がそれぞれ160ビットであるので、合計448ビットに対する電子署名を生成する。

【0112】Aの公開鍵証明書、Ra、Rb、Av、電子署名A.Sigを受信したBは、Aが送信してきたRbが、Bが生成したものと一致するか検証する。その結果、一致していた場合には、Aの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Aの公開鍵を取り出す。そして、取り出したAの公開鍵を用い電子署名A.

Sigを検証する。

【0113】次に、Bは、素数pより小さい乱数Bkを生成する。そして、ベースポイントGをBk倍した点Bv=Bk×Gを求め、Rb、Ra、Bv（X座標とY座標）に対する電子署名B.Sigを生成し、Bの公開鍵証明書とともにAに返送する。

【0114】Bの公開鍵証明書、Rb、Ra、Av、電子署名B.Sigを受信したAは、Bが送信してきたRaが、Aが生成したものと一致するか検証する。その結果、一致していた場合には、Bの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Bの公開鍵を取り出す。そして、取り出したBの公開鍵を用い電子署名B.Sigを検証する。電子署名の検証に成功した後、AはBを正当なものとして認証する。

【0115】両者が認証に成功した場合には、BはBk×Av（Bkは乱数だが、Avは楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要）を計算し、AはAk×Bvを計算し、これら点のX座標の下位64ビットをセッションキーとして以降の通信に使用する（共通鍵暗号を64ビット鍵長の共通鍵暗号とした場合）。もちろん、Y座標からセッション鍵を生成してもよいし、下位64ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッションキーで暗号化されるだけでなく、電子署名も付されることがある。

【0116】電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【0117】図16に公開鍵認証と有効化キープブロック（EKB）を使用したコンテンツキーの配信処理例を示す。まずコンテンツプロバイダとPC間において図15で説明した公開鍵方式による認証処理が実行される。コンテンツプロバイダは、コンテンツキー配信先である再生装置、記録媒体の有するノードキー、リーフキーによって復号可能なEKBを生成して、更新ノードキーによる暗号化を実行したコンテンツキーE(Kcon)と、有効化キープブロック（EKB）とをPC間の認証処理において生成したセッションキーKsesで暗号化してPCに送信する。

【0118】PCはセッションキーで暗号化された〔更新ノードキーによる暗号化を実行したコンテンツキーE(Kcon)と、有効化キープブロック（EKB）〕をセッションキーで復号した後、再生装置、記録媒体に送信する。

【0119】再生装置、記録媒体は、自身の保有するノードキーまたはリーフキーによって〔更新ノードキーによる暗号化を実行したコンテンツキーE(Kcon)と、有効化キープブロック（EKB）〕を復号することによってコンテンツキーKconを取得する。

【0120】この構成によれば、コンテンツプロバイダ

29

とPC間での認証を条件として[更新ノードキーによる暗号化を実行したコンテンツキーE (Kcon)と、有効化キーブロック(EKB)]が送信されるので、例えば、ノードキーの漏洩があった場合でも、確実な相手に対するデータ送信が可能となる。

【0121】[プログラムコードの有効化キーブロック(EKB)を使用した配信] 上述した例では、コンテンツキー、認証キー等を有効化キーブロック(EKB)を用いて暗号化して配信する方法を説明したが、様々なプログラムコードを有効化キーブロック(EKB)を用いて配信する構成も可能である。すなわちEKBによる暗号化メッセージデータをプログラムコードとした例である。以下、この構成について説明する。

【0122】図17にプログラムコードを有効化キーブロック(EKB)の例えば更新ノードキーによって暗号化してデバイス間で送信する例を示す。デバイス1701は、デバイス1702の有するノードキー、リーフキーによって復号可能な有効化キーブロック(EKB)と、有効化キーブロック(EKB)に含まれる更新ノードキーで暗号処理したプログラムコードをデバイス1702に送信する。デバイス1702は受信したEKBを処理して更新ノードキーを取得して、さらに取得した更新ノードキーによってプログラムコードの復号を実行して、プログラムコードを得る。

【0123】図17に示す例では、さらに、デバイス1702において取得したプログラムコードによる処理を実行して、その結果をデバイス1701に返して、デバイス1701がその結果に基づいて、さらに処理を続行する例を示している。

【0124】このように有効化キーブロック(EKB)と、有効化キーブロック(EKB)に含まれる更新ノードキーで暗号処理したプログラムコードを配信することにより、特定のデバイスにおいて解読可能なプログラムコードを前述の図3で示した特定のデバイス、あるいはグループに対して配信することが可能となる。

【0125】[送信コンテンツに対するチェック値(ICV: Integrity Check Value)を対応させる構成] 次に、コンテンツの改竄を防止するためにコンテンツのインテグリティ・チェック値(ICV)を生成して、コンテンツに対応付けて、ICVの計算により、コンテンツ改竄の有無を判定する処理構成について説明する。

【0126】コンテンツのインテグリティ・チェック値(ICV)は、例えばコンテンツに対するハッシュ関数を用いて計算され、 $ICV = hash(Kicv, C1, C2, \dots)$ によって計算される。KicvはICV生成キーである。C1, C2はコンテンツの情報であり、コンテンツの重要情報のメッセージ認証符号(MAC: Message authentication Code)が使用される。

【0127】DES暗号処理構成を用いたMAC値生成例を図18に示す。図18の構成に示すように対象とな

30

るメッセージを8バイト単位に分割し、(以下、分割されたメッセージをM1, M2, ..., MNとする)、まず、初期値(Initial Value (以下、IVとする))とM1を排他的論理和する(その結果をI1とする)。次に、I1をDES暗号化部に入れ、鍵(以下、K1とする)を用いて暗号化する(出力をE1とする)。続けて、E1およびM2を排他的論理和し、その出力I2をDES暗号化部へ入れ、鍵K1を用いて暗号化する(出力E2)。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたENがメッセージ認証符号(MAC (Message Authentication Code))となる。

【0128】このようなコンテンツのMAC値とICV生成キーにハッシュ関数を適用して用いてコンテンツのインテグリティ・チェック値(ICV)が生成される。改竄のないことが保証された例えばコンテンツ生成時に生成したICVと、新たにコンテンツに基づいて生成したICVとを比較して同一のICVが得られればコンテンツに改竄のないことが保証され、ICVが異なれば、改竄があったと判定される。

【0129】[チェック値(ICV)の生成キーKicvをEKBによって配布する構成] 次に、コンテンツのインテグリティ・チェック値(ICV)生成キーであるKicvを上記の有効化キーブロックによって送付する構成について説明する。すなわちEKBによる暗号化メッセージデータをコンテンツのインテグリティ・チェック値(ICV)生成キーとした例である。

【0130】図19および図20に複数のデバイスに共通のコンテンツを送付した場合、それらのコンテンツの改竄の有無を検証するためのインテグリティ・チェック値生成キーKicvを有効化キーブロック(EKB)によって配信する構成例を示す。図19はデバイス0, 1, 2, 3に対して復号可能なチェック値生成キーKicvを配信する例、図20はデバイス0, 1, 2, 3中のデバイス3をリボーク(排除)してデバイス0, 1, 2に対してのみ復号可能なチェック値生成キーKicvを配信する例を示す。

【0131】図19の例では、更新ノードキーK(t)00によって、チェック値生成キーKicvを暗号化したデータ(b)とともに、デバイス0, 1, 2, 3においてそれぞれの有するノードキー、リーフキーを用いて更新されたノードキーK(t)00を復号可能な有効化キーブロック(EKB)を生成して配信する。それぞれのデバイスは、図19の右側に示すようにまず、EKBを処理(復号)することにより、更新されたノードキーK(t)00を取得し、次に、取得したノードキーK(t)00を用いて暗号化されたチェック値生成キー: Enc(K(t)00, Kicv)を復号してチェック値生成キーKicvを得ることが可能となる。

【0132】その他のデバイス4, 5, 6, 7...は同一

31

の有効化キープブロック (EKB) を受信しても自身の保有するノードキー、リーフキーでは、EKBを処理して更新されたノードキー $K(t)00$ を取得することができないので、安全に正当なデバイスに対してのみチェック値生成キーを送付することができる。

【0133】一方、図20の例は、図3の点線枠で囲んだグループにおいてデバイス3が、例えば鍵の漏洩によりリボーク（排除）されているとして、他のグループのメンバ、すなわち、デバイス0, 1, 2, に対してのみ復号可能な有効化キープブロック (EKB) を生成して配信した例である。図20に示す (a) 有効化キープブロック (EKB) と、 (b) チェック値生成キー (Kicv) をノードキー ($K(t)00$) で暗号化したデータを配信する。

【0134】図20の右側には、復号手順を示してある。デバイス0, 1, 2は、まず、受領した有効化キープブロックから自身の保有するリーフキーまたはノードキーを用いた復号処理により、更新ノードキー ($K(t)00$) を取得する。次に、 $K(t)00$ による復号によりチェック値生成キー Kicv を取得する。

【0135】図3に示す他のグループのデバイス4, 5, 6…は、この同様のデータ (EKB) を受信したとしても、自身の保有するリーフキー、ノードキーを用いて更新ノードキー ($K(t)00$) を取得することができない。同様にリボークされたデバイス3においても、自身の保有するリーフキー、ノードキーでは、更新ノードキー ($K(t)00$) を取得することができず、正当な権利を有するデバイスのみがチェック値生成キーを復号して利用することが可能となる。

【0136】このように、EKBを利用したチェック値生成キーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能としたチェック値生成キーを配信することが可能となる。

【0137】このようなコンテンツのインテグリティ・チェック値 (ICV) を用いることにより、EKBと暗号化コンテンツの不正コピーを排除することができる。例えば図21に示すように、コンテンツC1とコンテンツC2とをそれぞれのコンテンツキーを取得可能な有効化キープブロック (EKB) とともに格納したメディア1があり、これをそのままメディア2にコピーした場合を想定する。EKBと暗号化コンテンツのコピーは可能であり、これをEKBを復号可能なデバイスでは利用できることになる。

【0138】図21の (b) に示すように各メディアに正当に格納されたコンテンツに対応付けてインテグリティ・チェック値 (ICV (C1, C2)) を格納する構成とする。なお、(ICV (C1, C2)) は、コンテンツC1とコンテンツC2にハッシュ関数を用いて計算されるコンテンツのインテグリティ・チェック値である $ICV = hash(Kicv, C1, C2)$ を示してい

32

る。図21の (b) の構成において、メディア1には正当にコンテンツ1とコンテンツ2が格納され、コンテンツC1とコンテンツC2に基づいて生成されたインテグリティ・チェック値 (ICV (C1, C2)) が格納される。また、メディア2には正当にコンテンツ1が格納され、コンテンツC1に基づいて生成されたインテグリティ・チェック値 (ICV (C1)) が格納される。この構成において、メディア1に格納された {EKB, コンテンツ2} をメディア2にコピーしたとすると、メディア2で、コンテンツチェック値を新たに生成すると ICV (C1, C2) が生成されることになり、メディアに格納されている Kicv (C1) と異なり、コンテンツの改竄あるいは不正なコピーによる新たなコンテンツの格納が実行されたことが明らかになる。メディアを再生するデバイスにおいて、再生ステップの前ステップに ICVチェックを実行して、生成ICVと格納ICVの一致を判別し、一致しない場合は、再生を実行しない構成とすることにより、不正コピーのコンテンツの再生を防止することが可能となる。

【0139】また、さらに、安全性を高めるため、コンテンツのインテグリティ・チェック値 (ICV) を書き換えカウンタを含めたデータに基づいて生成する構成としてもよい。すなわち $ICV = hash(Kicv, counter + 1, C1, C2, \dots)$ によって計算する構成とする。ここで、カウンタ (counter + 1) は、ICVの書き換えごとに1つインクリメントされる値として設定する。なお、カウンタ値はセキュアなメモリに格納する構成とすることが必要である。

【0140】さらに、コンテンツのインテグリティ・チェック値 (ICV) をコンテンツと同一メディアに格納することができない構成においては、コンテンツのインテグリティ・チェック値 (ICV) をコンテンツとは別のメディア上に格納する構成としてもよい。

【0141】例えば、読み込み専用メディアや通常のMO等のコピー防止策のとられていないメディアにコンテンツを格納する場合、同一メディアにインテグリティ・チェック値 (ICV) を格納すると ICVの書き換えが不正なユーザによりなされる可能性があり、ICVの安全性が保てないおそれがある。この様な場合、ホストマシン上の安全なメディアに ICVを格納して、コンテンツのコピーコントロール (例えばcheck-in/check-out、move) に ICVを使用する構成とすることにより、ICVの安全な管理およびコンテンツの改竄チェックが可能となる。

【0142】この構成例を図22に示す。図22では読み込み専用メディアや通常のMO等のコピー防止策のとられていないメディア2201にコンテンツが格納され、これらのコンテンツに関するインテグリティ・チェック値 (ICV) を、ユーザが自由にアクセスすることの許可されないホストマシン上の安全なメディア220

2に格納し、ユーザによる不正なインテグリティ・チェック値（ICV）の書き換えを防止した例である。このような構成として、例えばメディア2201を装着したデバイスがメディア2201の再生を実行する際にホストマシンであるPC、サーバにおいてICVのチェックを実行して再生の可否を判定する構成とすれば、不正なコピーコンテンツあるいは改竄コンテンツの再生を防止できる。

【0143】[階層ツリー構造のカテゴリ分類] 暗号鍵をルートキー、ノードキー、リーフキー等、図3の階層ツリー構造として構成し、コンテンツキー、認証キー、ICV生成キー、あるいはプログラムコード、データ等を有効化キーブロック（EKB）とともに暗号化して配信する構成について説明してきたが、ノードキー等を定義している階層ツリー構造を各デバイスのカテゴリ毎に分類して効率的なキー更新処理、暗号化キー配信、データ配信を実行する構成について、以下説明する。

【0144】図23に階層ツリー構造のカテゴリの分類の一例を示す。図23において、階層ツリー構造の最上段には、ルートキー-Kroot2301が設定され、以下の中間段にはノードキー2302が設定され、最下段には、リーフキー2303が設定される。各デバイスは個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーを保有する。

【0145】ここで、一例として最上段から第M段目のあるノードをカテゴリノード2304として設定する。すなわち第M段目のノードの各々を特定カテゴリのデバイス設定ノードとする。第M段の1つのノードを頂点として以下、M+1段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノードおよびリーフとする。

【0146】例えば図23の第M段目の1つのノード2305にはカテゴリ「メモリスティック（商標）」が設定され、このノード以下に連なるノード、リーフはメモリスティックを使用した様々なデバイスを含むカテゴリ専用のノードまたはリーフとして設定される。すなわち、ノード2305以下を、メモリスティックのカテゴリに定義されるデバイスの関連ノード、およびリーフの集合として定義する。

【0147】さらに、M段から数段分下位の段をサブカテゴリノード2306として設定することができる。例えば図に示すようにカテゴリ「メモリスティック」ノード2305の2段下のノードに、メモリスティックを使用したデバイスのカテゴリに含まれるサブカテゴリノードとして、[再生専用器]のノードを設定する。さらに、サブカテゴリノードである再生専用器のノード2306以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード2307が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる

[PHS] ノード2308と[携帯電話] ノード2309を設定することができる。

【0148】さらに、カテゴリ、サブカテゴリは、デバイスの種類のみならず、例えばあるメーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位（これらを総称して以下、エンティティと呼ぶ）で設定することが可能である。例えば1つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器XYZ専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器XYZにその頂点ノード以下の下段のノードキー、リーフキーを格納して販売することが可能となり、その後、暗号化コンテンツの配信、あるいは各種キーの配信、更新処理を、その頂点ノードキー以下のノードキー、リーフキーによって構成される有効化キーブロック（EKB）を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

【0149】このように、1つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の1つの頂点ノードを管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化キーブロック（EKB）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイスには全く影響を及ぼさずにキー更新を実行することができる。

【0150】[簡略EKBによるキー配信構成（1）] 先に説明した例えば図3のツリー構成において、キー、例えばコンテンツキーを所定デバイス（リーフ）宛に送付する場合、キー配布先デバイスの所有しているリーフキー、ノードキーを用いて復号可能な有効化キーブロック（EKB）を生成して提供する。例えば図24（a）に示すツリー構成において、リーフを構成するデバイスa, g, jに対してキー、例えばコンテンツキーを送信する場合、a, g, jの各ノードにおいて復号可能な有効化キーブロック（EKB）を生成して配信する。

【0151】例えば更新ルートキーK(t)rootでコンテンツキーK(t)conを暗号化処理し、EKBとともに配信する場合を考える。この場合、デバイスa, g, jは、それぞれが図24（b）に示すリーフおよびノードキーを用いて、EKBの処理を実行してK(t)rootを取得し、取得した更新ルートキーK(t)rootによってコンテンツキーK(t)conの復号処理を実行してコンテンツキーを得る。

【0152】この場合に提供される有効化キーブロック（EKB）の構成は、図25に示すようになる。図25に示す有効化キーブロック（EKB）は、先の図6で説

明した有効化キープブロック (EKB) のフォーマットにしたがって構成されたものであり、データ (暗号化キー) と対応するタグとを持つ。タグは、先に図7を用いて説明したように左 (L)、右 (R)、それぞれの方向にデータがあれば0、無ければ1を示している。

【0153】有効化キープブロック (EKB) を受領したデバイスは、有効化キープブロック (EKB) の暗号化キーとタグに基づいて、順次暗号化キーの復号処理を実行して上位ノードの更新キーを取得していく。図25に示すように、有効化キープブロック (EKB) は、ルートからリーフまでの段数 (デプス) が多いほど、そのデータ量は増加していく。段数 (デプス) は、デバイス (リーフ) 数に応じて増大するものであり、キーの配信先となるデバイス数が多い場合は、EKBのデータ量がさらに増大することになる。

【0154】このような有効化キープブロック (EKB) のデータ量の削減を可能とした構成について説明する。図26は、有効化キープブロック (EKB) をキー配信デバイスに応じて簡略化して構成した例を示すものである。

【0155】図25と同様、リーフを構成するデバイス a, g, j に対してキー、例えばコンテンツキーを送信する場合を想定する。図26の (a) に示すように、キー配信デバイスによってのみ構成されるツリーを構築する。この場合、図24 (b) に示す構成に基づいて新たなツリー構成として図26 (b) のツリー構成が構築される。K root から K j までは全く分岐がなく1つの枝のみが存在すればよく、K root から K a および K g に至るためには、K 0 に分岐点を構成するのみで、2分岐構成の図26 (a) のツリーが構築される。

【0156】図26 (a) に示すように、ノードとして K 0 のみを持つ簡略化したツリーが生成される。更新キー配信のための有効化キープブロック (EKB) は、これらの簡略ツリーに基づいて生成する。図26 (a) に示すツリーは、有効化キープブロック (EKB) を復号可能な末端ノードまたはリーフを最下段とした2分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーである。更新キー配信のための有効化キープブロック (EKB) は、この再構築階層ツリーのノードまたはリーフに対応するキーのみに基づいて構成される。

【0157】先の図25で説明した有効化キープブロック (EKB) は、各リーフ a, g, j から K root に至るまでのすべてのキーを暗号化したデータを格納していたが、簡略化EKBは、簡略化したツリーを構成するノードについてのみの暗号化データを格納する。図26

(b) に示すようにタグは3ビット構成を有する。第1および第2ビットは、図25の例と、同様の意味を持ち、左 (L)、右 (R)、それぞれの方向にデータがあれば0、無ければ1を示す。第3番目のビットは、E

B内に暗号化キーが格納されているか否かを示すためのビットであり、データが格納されている場合は1、データが無い場合は、0として設定される。

【0158】データ通信網、あるいは記憶媒体に格納されてデバイス (リーフ) に提供される有効化キープブロック (EKB) は、図26 (b) に示すように、図25に示す構成に比較すると、データ量が大幅に削減されたものとなる。図26に示す有効化キープブロック (EKB) を受領した各デバイスは、タグの第3ビットに1が格納された部分のデータのみを順次復号することにより、所定の暗号化キーの復号を実現することができる。例えばデバイス a は、暗号化データ Enc (K a, K (t) 0) をリーフキー K a で復号して、ノードキー K (t) 0 を取得して、ノードキー K (t) 0 によって暗号化データ Enc (K (t) 0, K (t) root) を復号して K (t) root を取得する。デバイス j は、暗号化データ Enc (K j, K (t) root) をリーフキー K j で復号して、K (t) root を取得する。

【0159】このように、配信先のデバイスによってのみ構成される簡略化した新たなツリー構成を構築して、構築されたツリーを構成するリーフおよびノードのキーのみを用いて有効化キープブロック (EKB) を生成することにより、少ないデータ量の有効化キープブロック (EKB) を生成することが可能となり、有効化キープブロック (EKB) のデータ配信が効率的に実行可能となる。

【0160】[簡略EKBによるキー配信構成 (2)] 図26で示した簡略化したツリーに基づいて生成される有効化キープブロック (EKB) をさらに、簡略化してデータ量を削減し、効率的な処理を可能とした構成について説明する。

【0161】図26を用いて説明した構成は、有効化キープブロック (EKB) を復号可能な末端ノードまたはリーフを最下段とした2分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーであった。更新キー配信のための有効化キープブロック (EKB) は、この再構築階層ツリーのノードまたはリーフに対応するキーのみに基づいて構成される。

【0162】図26 (a) に示す再構築階層ツリーは、リーフ a, g, j において更新ルートキー K (t) root を取得可能とするため、図26 (b) に示す有効化キープブロック (EKB) を配信する。図26 (b) の有効化キープブロック (EKB) の処理において、リーフ j は、Enc (K j, K (t) root) の1回の復号処理によりルートキー: K (t) root を取得できる。しかし、リーフ a, g は、Enc (K a, K (t) 0) または、Enc (K g, K (t) 0) の復号処理により K (t) 0 を得た後、さらに、Enc (K (t) 0, K (t) root) の復号処理を実行してルートキー: K (t) root を取得する。すなわち、リーフ a, g

37

は、2回の復号処理を実行することが必要となる。

【0163】図26の簡略化した再構築階層ツリーは、ノードK0がその下位リーフa、gの管理ノードとして独自の管理を実行している場合、例えば後述するサブルート・ノードとして、下位リーフの管理を実行している場合には、リーフa、gが更新キーを取得したことを確認する意味で有効であるが、ノードK0が下位リーフの管理を行っていない場合、あるいは行なっていたとしても、上位ノードからの更新キー配信を許容している場合には、図26(a)に示す再構築階層ツリーをさらに簡略化して、ノードK0のキーを省略して有効化キープブロック(EKB)を生成して配信してもよい。

【0164】図27に、このような有効化キープブロック(EKB)の構成を示す。図26と同様、リーフを構成するデバイスa、g、jに対してキー、例えばコンテンツキーを送信する場合を想定する。図27の(a)に示すように、ルートKrootと各リーフa、g、jを直接接続したツリーを構築する。

【0165】図27(a)に示すように、図26(a)に示す再構築階層ツリーからノードK0が省かれた簡略化されたツリーが生成される。更新キー配信のための有効化キープブロック(EKB)は、これらの簡略ツリーに基づいて生成する。図27(a)に示すツリーは、有効化キープブロック(EKB)を復号可能なリーフをとルートとを直接結ぶパスのみによって再構築される再構築階層ツリーである。更新キー配信のための有効化キープブロック(EKB)は、この再構築階層ツリーのリーフに対応するキーのみに基づいて構成される。

【0166】なお、図27(a)の例は、末端をリーフとした構成例であるが、例えば最上位ノードか複数の中位、下位ノードに対してキーを配信する場合も、最上位ノードと中位、下位ノードとを直接接続した簡略化ツリーに基づいて有効化キープブロック(EKB)を生成してキー配信を実行することが可能である。このように、再構築階層ツリーは、簡略化したツリーを構成する頂点ノードと、簡略化したツリーを構成する末端ノードまたはリーフとを直接、接続した構成を持つ。この簡略化ツリーでは、頂点ノードからの分岐は2に限らず、配信ノードまたはリーフ数に応じて3以上の多分岐を持つツリーとして構成することが可能である。

【0167】先の図25で説明した有効化キープブロック(EKB)は、各リーフa、g、jからKrootに至るまでのすべてのキーを暗号化したデータを格納し、図26で説明した有効化キープブロック(EKB)は、リーフa、g、jのリーフキー、a、gの共通ノードとしてのK0、さらに、ルートキーを格納した構成であったが、図27(a)に示す簡略化階層ツリーに基づく有効化キープブロック(EKB)は、ノードK0のキーを省略したので、図27(b)に示すように、さらにデータ量の少ない有効化キープブロック(EKB)となる。

38

【0168】図27(b)の有効化キープブロック(EKB)は、図26(b)の有効化キープブロック(EKB)と同様、3ビット構成のタグを有する。第1および第2ビットは、図26で説明したと同様、左(L)、右(R)、それぞれの方向にデータがあれば0、無ければ1を示す。第3番目のビットは、EKB内に暗号化キーが格納されているか否かを示すためのビットであり、データが格納されている場合は1、データが無い場合は、0として設定される。

10 【0169】図27(b)の有効化キープブロック(EKB)において、各リーフa、g、jは、 $Enc(Ka, K(t)root)$ 、または $Enc(Kg, K(t)root)Enc(Kj, K(t)root)$ の1回の復号処理によりルートキー： $K(t)root$ を取得できる。

【0170】このように簡略化された再構築ツリーの最上位ノードと、ツリーを構成する末端ノードまたはリーフとを直接、接続した構成を持つツリーに基づいて生成される有効化キープブロック(EKB)は、図27(b)に示すように、再構築階層ツリーの頂点ノードおよび末端ノードまたはリーフに対応するキーのみに基づいて構成される。

【0171】図26または図27で説明した有効化キープブロック(EKB)のように、配信先のデバイスによってのみ構成される簡略化された新たなツリー構成を構築して、構築されたツリーを構成するリーフのみ、あるいはリーフと共通ノードのキーのみを用いて有効化キープブロック(EKB)を生成することにより、少ないデータ量の有効化キープブロック(EKB)を生成することが可能となり、有効化キープブロック(EKB)のデータ配信が効率的に実行可能となる。

【0172】なお、簡略化した階層ツリー構成は、後段で説明するエンティティ単位のEKB管理構成において特に有効に活用可能である。エンティティは、キー配信構成としてのツリー構成を構成するノードあるいはリーフから選択した複数のノードあるいはリーフの集合体ブロックである。エンティティは、デバイスの種類に応じて設定される集合であったり、あるいはデバイス提供メーカー、コンテンツプロバイダ、決済機関等の管理単位等、ある共通点を持った処理単位、管轄単位、あるいは提供サービス単位等、様々な態様の集合として設定される。1つのエンティティには、ある共通のカテゴリに分類されるデバイスが集まっており、例えば複数のエンティティの頂点ノード(サブルート)によって上述したと同様の簡略化したツリーを再構築してEKBを生成することにより、選択されたエンティティに属するデバイスにおいて復号可能な簡略化された有効化キープブロック(EKB)の生成、配信が可能となる。エンティティ単位の管理構成については後段で詳細に説明する。

50 【0173】なお、このような有効化キープブロック(E

39

KB) は、光ディスク、DVD等の情報記録媒体に格納した構成とすることが可能である。例えば、上述の暗号化キーデータによって構成されるデータ部と、暗号化キーデータの階層ツリー構造における位置識別データとしてのタグ部とを含む有効化キープロック (EKB) にさらに、更新ノードキーによって暗号化したコンテンツ等のメッセージデータとを格納した情報記録媒体を各デバイスに提供する構成が可能である。デバイスは有効化キープロック (EKB) に含まれる暗号化キーデータをタグ部の識別データにしたがって順次抽出して復号し、コンテンツの復号に必要なキーを取得してコンテンツの利用を行なうことが可能となる。もちろん、有効化キープロック (EKB) をインターネット等のネットワークを介して配信する構成としてもよい。

【0174】 [エンティティ単位のEKB管理構成] 次に、キー配信構成としてのツリー構成を構成するノードあるいはリーフを、複数のノードあるいはリーフの集合としてのブロックで管理する構成について説明する。なお、複数のノードあるいはリーフの集合としてのブロックを以下エンティティと呼ぶ。エンティティは、デバイスの種類に応じて設定される集合であったり、あるいはデバイス提供メーカー、コンテンツプロバイダ、決済機関等の管理単位等、ある共通点を持った処理単位、管轄単位、あるいは提供サービス単位等、様々な態様の集合として設定される。

【0175】 エンティティについて、図28を用いて説明する。図28(a) はツリーのエンティティ単位での管理構成を説明する図である。1つのエンティティは図では、三角形として示し、例えば1エンティティ2701内には、複数のノードが含まれる。1エンティティ内のノード構成を示すのが(b)である。1つのエンティティは、1つのノードを頂点とした複数段の2分岐形ツリーによって構成される。以下、エンティティの頂点ノード2702をサブルートと呼ぶ。

【0176】 ツリーの末端は、(c)に示すようにリーフ、すなわちデバイスによって構成される。デバイスは、複数デバイスをリーフとし、サブルートである頂点ノード2702を持つツリーによって構成されるいずれかのエンティティに属する。

【0177】 図28(a) から理解されるように、エンティティは、階層構造を持つ。この階層構造について、図29を用いて説明する。

【0178】 図29(a) は、階層構造を簡略化して説明するための図であり、K r o o t から数段下の段にエンティティA01~Annが構成され、エンティティA1~Anの下位には、さらに、エンティティB01~Bnk、さらに、その下位にエンティティC1~Cnqが設定されている。各エンティティは、図29(b)、

(c)に示す如く、複数段のノード、リーフによって構成されるツリー形状を持つ。

40

【0179】 例えばエンティティBnkの構成は、

(b)に示すように、サブルート2811を頂点ノードとして、末端ノード2812に至るまでの複数ノードを有する。このエンティティは識別子Bnkを持ち、エンティティBnk内のノードに対応するノードキー管理をエンティティBnk独自に実行することにより、末端ノード2812を頂点として設定される下位(子)エンティティの管理を実行する。また、一方、エンティティBnkは、サブルート2811を末端ノードとして持つ上位(親)エンティティAnnの管理下にある。

【0180】 エンティティCn3の構成は、(c)に示すように、サブルート2851を頂点ノードとして、各デバイスである末端ノード2852、この場合はリーフに至るまで複数ノード、リーフを有する。このエンティティは識別子Cn3を持ち、エンティティCn3内のノード、リーフに対応するノードキー、リーフキー管理をエンティティCn3独自に実行することにより、末端ノード2852に対応するリーフ(デバイス)の管理を実行する。また、一方、エンティティCn3は、サブルート2851を末端ノードとして持つ上位(親)エンティティBn2の管理下にある。各エンティティにおけるキー管理とは、例えばキー更新処理、リポーク処理等であるが、これらは後段で詳細に説明する。

【0181】 最下段エンティティのリーフであるデバイスには、デバイスの属するエンティティのリーフキーから、自己の属するエンティティの頂点ノードであるサブルートノードに至るパスに位置する各ノードのノードキーおよびリーフキーが格納される。例えば末端ノード2852のデバイスは、末端ノード(リーフ)2852から、サブルートノード2851までの各キーを格納する。

【0182】 図30を用いて、さらにエンティティの構成について説明する。エンティティは様々な段数によって構成されるツリー構造を持つことが可能である。段数、すなわちデプス(depth)は、エンティティで管理する末端ノードに対応する下位(子)エンティティの数、あるいはリーフとしてのデバイス数に応じて設定可能である。

【0183】 図30の(a)に示すような上下エンティティ構成を具体化すると、(b)に示す態様となる。ルートエンティティは、ルートキーを持つ最上段のエンティティである。ルートエンティティの末端ノードに複数の下位エンティティとしてエンティティA、B、Cが設定され、さらに、エンティティCの下位エンティティとしてエンティティDが設定される。エンティティC2901は、その末端ノードの1つ以上のノードをリザーブノード2950として保持し、自己の管理するエンティティを増加させる場合、さらに複数段のツリー構成を持つエンティティC'2902をリザーブノード2950を頂点ノードとして新設することにより、管理末端ノ

41

ド2970を増加させて、管理末端ノードに増加した下位エンティティを追加することができる。

【0184】リザーブノードについて、さらに図31を用いて説明する。エンティティA、3011は、管理する下位エンティティB、C、D…を持ち、1つのリザーブノード3021を持つ。エンティティは管理対象の下位エンティティをさらに増加させたい場合、リザーブノード3021に、自己管理の下位エンティティA'、3012を設定し、下位エンティティA'、3012の末端ノードにさらに管理対象の下位エンティティF、Gを設定することができる。自己管理の下位エンティティA'、3012も、その末端ノードの少なくとも1つをリザーブノード3022として設定することにより、さらに下位エンティティA''、3013を設定して、さらに管理エンティティを増加させることができる。下位エンティティA''、3013の末端ノードにも1以上のリザーブノードを確保する。このようなリザーブノード保有構成をとることにより、あるエンティティの管理する下位エンティティは、際限なく増加させることが可能となる。なお、リザーブエンティティは、末端ノードの1つのみではなく、複数個設定する構成としてもよい。

【0185】それぞれのエンティティでは、エンティティ単位で有効化キープブロック(EKB)が構成され、エンティティ単位でのキー更新、リポーク処理を実行することになる。図31のように複数のエンティティA、A'、A''には各エンティティ個々の有効化キープブロック(EKB)が設定されることになるが、これらは、エンティティA、A'、A''を共通に管理する例えばあるデバイスメーカーが一括して管理することが可能である。

【0186】[新規エンティティの登録処理]次に、新規エンティティの登録処理について説明する。登録処理シーケンスを図32に示す。図32のシーケンスにしたがって説明する。新たにツリー構成中に追加される新規(子)エンティティ(N-En)は、上位(親)エンティティ(P-En)に対して新規登録要求を実行する。なお、各エンティティは、公開鍵暗号方式に従った公開鍵を保有し、新規エンティティは自己の公開鍵を登録要求に際して上位エンティティ(P-En)に送付する。

【0187】登録要求を受領した上位エンティティ(P-En)は、受領した新規(子)エンティティ(N-En)の公開鍵を証明書発行局(CA: Certificate Authority)に転送し、CAの署名を付加した新規(子)エンティティ(N-En)の公開鍵を受領する。これらの手続きは、上位エンティティ(P-En)と新規(子)エンティティ(N-En)との相互認証の手続きとして行われる。

【0188】これらの処理により、新規登録要求エンティティの認証が終了すると、上位エンティティ(P-En)は、新規(子)エンティティ(N-En)の登録を

42

許可し、新規(子)エンティティ(N-En)のノードキーを新規(子)エンティティ(N-En)に送信する。このノードキーは、上位エンティティ(P-En)の末端ノードの1つのノードキーであり、かつ、新規(子)エンティティ(N-En)の頂点ノード、すなわちサブルートキーに対応する。

【0189】このノードキー送信が終了すると、新規(子)エンティティ(N-En)は、新規(子)エンティティ(N-En)のツリー構成を構築し、構築したツリーの頂点に受信した頂点ノードのサブルートキーを設定し、各ノード、リーフのキーを設定して、エンティティ内の有効化キープブロック(EKB)を生成する。1つのエンティティ内の有効化キープブロック(EKB)をサブEKBと呼ぶ。

【0190】一方、上位エンティティ(P-En)は、新規(子)エンティティ(N-En)の追加により、有効化する末端ノードを追加した上位エンティティ(P-En)内のサブEKBを生成する。

【0191】新規(子)エンティティ(N-En)は、新規(子)エンティティ(N-En)内のノードキー、リーフキーによって構成されるサブEKBを生成すると、これを上位エンティティ(P-En)に送信する。

【0192】新規(子)エンティティ(N-En)からサブEKBを受信した上位エンティティ(P-En)は、受信したサブEKBと、上位エンティティ(P-En)の更新したサブEKBとをキー発行センター(KDC: Key Distribute Center)に送信する。

【0193】キー発行センター(KDC)は、すべてのエンティティのサブEKBに基づいて、様々な態様のEKB、すなわち特定のエンティティあるいはデバイスのみが復号可能なEKBを生成することが可能となる。このように復号可能なエンティティあるいはデバイスを設定したEKBを例えばコンテンツプロバイダに提供し、コンテンツプロバイダがEKBに基づいてコンテンツキーを暗号化して、ネットワークを介して、あるいは記録媒体に格納して提供することにより、特定のデバイスでのみ利用可能なコンテンツを提供することが可能となる。

【0194】なお、新規エンティティのサブEKBのキー発行センター(KDC)に対する登録処理は、サブEKBを上位エンティティを介してを順次転送して実行する方法に限るものではなく、上位エンティティを介さずに、新規登録エンティティから直接、キー発行センター(KDC)に登録する処理を実行する構成としてもよい。

【0195】上位エンティティと、上位エンティティに新規追加する下位エンティティとの対応について図33を用いて説明する。上位エンティティの末端ノードの1つ3201を新規追加エンティティの頂点ノードとして、下位エンティティに提供することによって下位エン

ティティは、上位エンティティの管理下のエンティティとして追加される。上位エンティティの管理下のエンティティとは、後段で詳細に説明するが、下位エンティティのリボーク（排除）処理を上位エンティティが実行できる構成であるという意味を含むものである。

【0196】図33に示すように、上位エンティティに新規エンティティが設定されると、上位エンティティのリーフである末端ノードの1つのノード3201と新規追加エンティティの頂点ノード3202とが等しいノードとして設定される。すなわち上位ノードの1つのリーフである1つの末端ノードが、新規追加エンティティのサブルートとして設定される。このように設定されることにより、新規追加エンティティが全体ツリー構成の下で有効化される。

【0197】図34に新規追加エンティティを設定した際に上位エンティティが生成する更新EKBの例を示す。図34は、(a)に示す構成、すなわち既に有効に存在する末端ノード（node000）3301と末端ノード（node001）3302があり、ここに新規追加エンティティに新規エンティティ追加末端ノード

（node100）3303を付与した際に上位エンティティが生成するサブEKBの例を示したものである。

【0198】サブEKBは、図34の(b)に示すような構成を持つ。それぞれ有効に存在する末端ノードキーにより暗号化された上位ノードキー、上位ノードキーで暗号化されたさらなる上位ノードキー、…さらに上位に進行してサブルートキーに至る構成となっている。この構成によりサブEKBが生成される。各エンティティは図34(b)に示すと同様、有効な末端ノード、あるいはリーフキーにより暗号化された上位ノードキー、上位ノードキーでさらに上位のノードキーを暗号化し、順次上位に深厚してサブルートに至る暗号化データによって構成されるEKBを有し、これを管理する。

【0199】[エンティティ管理下におけるリボーク処理]次に、キー配信ツリー構成をエンティティ単位として管理する構成におけるデバイスあるいはエンティティのリボーク（排除）処理について説明する。先の図3、4では、ツリー構成全体の中から特定のデバイスのみ復号可能で、リボークされたデバイスは復号不可能な有効化キープロック（EKB）を配信する処理について説明した。図3、4で説明したリボーク処理は、ツリー全体の中から特定のリーフであるデバイスをリボークする処理であったが、ツリーのエンティティ管理による構成では、エンティティ毎にリボーク処理が実行可能となる。

【0200】図35以下の図を用いてエンティティ管理下のツリー構成におけるリボーク処理について説明する。図35は、ツリーを構成するエンティティのうち、最下段のエンティティ、すなわち個々のデバイスを管理しているエンティティによるデバイスのリボーク処理を説明する図である。

【0201】図35(a)は、エンティティ管理によるキー配信ツリー構造を示している。ツリー最上位にはルートノードが設定され、その数段下にエンティティA01～Ann、さらにその下位段にB01～Bnkのエンティティ、さらにその下位段にC1～cnのエンティティが構成されている。最下段のエンティティは、末端ノード（リーフ）が個々のデバイス、例えば記録再生器、再生専用器等であるとする。

【0202】ここで、リボーク処理は、各エンティティにおいて独自に実行される。例えば、最下段のエンティティC1～Cnでは、リーフのデバイスのリボーク処理が実行される。図35(b)には、最下段のエンティティの1つであるエンティティCn、3430のツリー構成を示している。エンティティCn、3430は、頂点ノード3431を持ち、末端ノードであるリーフに複数のデバイスを持つ構成である。

【0203】この末端ノードであるリーフ中に、リボーク対象となるデバイス、例えばデバイス3432があったとすると、エンティティCn、3430は、独自に更新したエンティティCn内のノードキー、リーフキーによって構成される有効化キープロック（サブEKB）を生成する。この有効化キープロックは、リボークデバイス3432においては復号できず、他のリーフを構成するデバイスにおいてのみ復号可能な暗号化キーにより構成されるキープロックである。エンティティCnの管理者は、これを更新されたサブEKBとして生成する。具体的には、サブルートからリボークデバイス3432に連なるパスを構成する各ノード3431、3434、3435のノードキーを更新して、この更新ノードキーをリボークデバイス3432以外のリーフデバイスにおいてのみ復号可能な暗号化キーとして構成したブロックを更新サブEKBとする。この処理は、先の図3、4において説明したリボーク処理構成において、ルートキーを、エンティティの頂点キーであるサブルートキーに置き換えた処理に対応する。

【0204】このようにエンティティCn、3430がリボーク処理によって更新した有効化キープロック（サブEKB）は、上位エンティティに送信される。この場合、上位エンティティはエンティティBnk、3420であり、エンティティCn、3430の頂点ノード3431を末端ノードとして有するエンティティである。

【0205】エンティティBnk、3420は、下位エンティティCn、3430から有効化キープロック（サブEKB）を受領すると、そのキープロックに含まれるエンティティCnk、3430の頂点ノード3431に対応するエンティティBnk、3420の末端ノード3431を、下位エンティティCn、3430において更新されたキーに設定して、自身のエンティティBnk、3420のサブEKBの更新処理を実行する。図35

(c)にエンティティBnk、3420のツリー構成を

45

示す。エンティティBnk, 3420において、更新対象となるノードキーは、図35(c)のサブルート3421からリポーカデバイスを含むエンティティを構成する末端ノード3431に至るパス上のノードキーである。すなわち、更新サブEKBを送信してきたエンティティのノード3431に連なるパスを構成する各ノード3421, 3424, 3425のノードキーが更新対象となる。これら各ノードのノードキーを更新してエンティティBnk, 3420の新たな更新サブEKBを生成する。

【0206】さらに、エンティティBnk, 3420が更新した有効化キーブロック(サブEKB)は、上位エンティティに送信される。この場合、上位エンティティはエンティティAnn, 3410であり、エンティティBnk, 3420の頂点ノード3421を末端ノードとして有するエンティティである。

【0207】エンティティAnn, 3410は、下位エンティティBnk, 3420から有効化キーブロック(サブEKB)を受領すると、そのキーブロックに含まれるエンティティBnk, 3420の頂点ノード3421に対応するエンティティAnn, 3410の末端ノード3421を、下位エンティティBnk, 3420において更新されたキーに設定して、自身のエンティティAnn, 3410のサブEKBの更新処理を実行する。図35(d)にエンティティAnn, 3410のツリー構成を示す。エンティティAnn, 3410において、更新対象となるノードキーは、図35(d)のサブルート3411から更新サブEKBを送信してきたエンティティのノード3421に連なるパスを構成する各ノード3411, 3414, 3415のノードキーである。これら各ノードのノードキーを更新してエンティティAnn, 3410の新たな更新サブEKBを生成する。

【0208】これらの処理を順次、上位のエンティティにおいて実行し、図30(b)で説明したルートエンティティまで実行する。この一連の処理により、デバイスのリポーカ処理が完結する。なお、それぞれのエンティティにおいて更新されたサブEKBは、最終的にキー発行センター(KDC)に送信され、保管される。キー発行センター(KDC)は、すべてのエンティティの更新サブEKBに基づいて、様々なEKBを生成する。更新EKBは、リポーカされたデバイスでの復号が不可能な暗号化キーブロックとなる。

【0209】デバイスのリポーカ処理のシーケンス図を図36に示す。処理手順を図36のシーケンス図に従って説明する。まず、ツリー構成の最下段にあるデバイス管理エンティティ(D-En)は、デバイス管理エンティティ(D-En)内のリポーカ対象のリーフを排除するために必要なキー更新を行ない、デバイス管理エンティティ(D-En)の新たなサブEKB(D)を生成する。更新サブEKB(D)は、上位エンティティに送付

46

される。更新サブEKB(D)を受領した上位(親)エンティティ(P1-En)は、更新サブEKB(D)の更新頂点ノードに対応した末端ノードキーの更新および、その末端ノードからサブルートに至るパス上のノードキーを更新した更新サブEKB(P1)を生成する。これらの処理を順次、上位エンティティにおいて実行して、最終的に更新されたすべてのサブEKBがキー発行センター(KDC)に格納され管理される。

【0210】図37にデバイスのリポーカ処理によって上位エンティティが更新処理を行なって生成する有効化キーブロック(EKB)の例を示す。

【0211】図37は、(a)に示す構成において、リポーカデバイスを含む下位エンティティから更新サブEKBを受信した上位エンティティにおいて生成するEKBの例を説明する図である。リポーカデバイスを含む下位エンティティの頂点ノードは、上位エンティティの末端ノード(node100)3601に対応する。

【0212】上位エンティティは、上位エンティティのサブルートから末端ノード(node100)3601までのパスに存在するノードキーを更新して新たな更新サブEKBを生成する。更新サブEKBは、図37

(b)のようになる。更新されたキーは、下線および「'」を付して示してある。このように更新された末端ノードからサブルートまでのパス上のノードキーを更新してそのエンティティにおける更新サブEKBとする。

【0213】次に、リポーカする対象をエンティティとした場合の処理、すなわちエンティティのリポーカ処理について説明する。

【0214】図38(a)は、エンティティ管理によるキー配信ツリー構造を示している。ツリー最上位にはルートノードが設定され、その数段下にエンティティA01~Ann、さらにその下位段にB01~Bnkのエンティティ、さらにその下位段にC1~cnのエンティティが構成されている。最も下のエンティティは、末端ノード(リーフ)が個々のデバイス、例えば記録再生器、再生専用器等であるとする。

【0215】ここで、リポーカ処理を、エンティティCn, 3730に対して実行する場合について説明する。最下段のエンティティCn, 3730は、図38(b)に示すように頂点ノード3431を持ち、末端ノードであるリーフに複数のデバイスを持つ構成である。

【0216】エンティティCn, 3730をリポーカすることにより、エンティティCn, 3730に属するすべてのデバイスのツリー構造からの一括排除が可能となる。エンティティCn, 3730のリポーカ処理は、エンティティCn, 3730の上位エンティティであるエンティティBnk, 3720において実行される。エンティティBnk, 3720は、エンティティCn, 3730の頂点ノード3731を末端ノードとして有するエ

47

ンティティである。

【0217】エンティティBnk, 3720は、下位エンティティCn, 3730のリポークを実行する場合、エンティティCnk, 3730の頂点ノード3731に対応するエンティティBnk, 3720の末端ノード3731を更新し、さらに、そのリポークエンティティ3730からエンティティBnk, 3720のサブルートまでのパス上のノードキーの更新を行ない有効化キープブロックを生成して更新サブEKBを生成する。更新対象となるノードキーは、図38(c)のサブルート3721からリポークエンティティの頂点ノードを構成する末端ノード3731に至るパス上のノードキーである。すなわち、ノード3721, 3724, 3725, 3731のノードキーが更新対象となる。これら各ノードのノードキーを更新してエンティティBnk, 3720の新たな更新サブEKBを生成する。

【0218】あるいは、エンティティBnk, 3720は、下位エンティティCn, 3730のリポークを実行する場合、エンティティCnk, 3730の頂点ノード3731に対応するエンティティBnk, 3720の末端ノード3731は更新せず、そのリポークエンティティ3730からエンティティBnk, 3720のサブルートまでのパス上の末端ノード3731を除くノードキーの更新を行ない有効化キープブロックを生成して更新サブEKBを生成してもよい。

【0219】さらに、エンティティBnk, 3720が更新した有効化キープブロック(サブEKB)は、上位エンティティに送信される。この場合、上位エンティティはエンティティAnn, 3710であり、エンティティBnk, 3720の頂点ノード3721を末端ノードとして有するエンティティである。

【0220】エンティティAnn, 3710は、下位エンティティBnk, 3720から有効化キープブロック(サブEKB)を受領すると、そのキープブロックに含まれるエンティティBnk, 3720の頂点ノード3721に対応するエンティティAnn, 3710の末端ノード3721を、下位エンティティBnk, 3720において更新されたキーに設定して、自身のエンティティAnn, 3710のサブEKBの更新処理を実行する。図38(d)にエンティティAnn, 3710のツリー構成を示す。エンティティAnn, 3710において、更新対象となるノードキーは、図38(d)のサブルート3711から更新サブEKBを送信してきたエンティティのノード3721に連なるパスを構成する各ノード3711, 3714, 3715のノードキーである。これら各ノードのノードキーを更新してエンティティAnn, 3710の新たな更新サブEKBを生成する。

【0221】これらの処理を順次、上位のエンティティにおいて実行し、図30(b)で説明したルートエンティティまで実行する。この一連の処理により、エンティ

48

ティのリポーク処理が完結する。なお、それぞれのエンティティにおいて更新されたサブEKBは、最終的にキー発行センター(KDC)に送信され、保管される。キー発行センター(KDC)は、すべてのエンティティの更新サブEKBに基づいて、様々なEKBを生成する。更新EKBは、リポークされたエンティティに属するデバイスでの復号が不可能な暗号化キープブロックとなる。

【0222】エンティティのリポーク処理のシーケンス図を図39に示す。処理手順を図39のシーケンス図に従って説明する。まず、エンティティをリポークしようとするエンティティ管理エンティティ(E-En)は、エンティティ管理エンティティ(E-En)内のリポーク対象の末端ノードを排除するために必要なキー更新を行ない、エンティティ管理エンティティ(E-En)の新たなサブEKB(E)を生成する。更新サブEKB

(E)は、上位エンティティに送付される。更新サブEKB(E)を受領した上位(親)エンティティ(P1-En)は、更新サブEKB(E)の更新頂点ノードに対応した末端ノードキーの更新および、その末端ノードからサブルートに至るパス上のノードキーを更新した更新サブEKB(P1)を生成する。これらの処理を順次、上位エンティティにおいて実行して、最終的に更新されたすべてのサブEKBがキー発行センター(KDC)に格納され管理される。キー発行センター(KDC)は、すべてのエンティティの更新サブEKBに基づいて、様々なEKBを生成する。更新EKBは、リポークされたエンティティに属するデバイスでの復号が不可能な暗号化キープブロックとなる。

【0223】図40にリポークされた下位エンティティと、リポークを行なった上位エンティティの対応を説明する図を示す。上位エンティティの末端ノード3901は、エンティティのリポークにより更新され、上位エンティティのツリーにおける末端ノード3901からサブルートまでのパスに存在するノードキーの更新により、新たなサブEKBが生成される。その結果、リポークされた下位エンティティの頂点ノード3902のノードキーと、上位エンティティの末端ノード3901のノードキーは不一致となる。エンティティのリポーク後にキー発行センター(KDC)によって生成されるEKBは、上位エンティティにおいて更新された末端ノード3901のキーに基づいて生成されることになるので、その更新キーを保有しない下位エンティティのリーフに対応するデバイスは、キー発行センター(KDC)によって生成されるEKBの復号が不可能になる。

【0224】なお、上述の説明では、デバイスを管理する最下段のエンティティのリポーク処理について説明したが、ツリーの中段にあるエンティティ管理エンティティをその上位エンティティがリポークする処理も上記と同様のプロセスによって可能である。中段のエンティティ管理エンティティをリポークすることにより、リポー

クされたエンティティ管理エンティティの下位に属するすべての複数エンティティおよびデバイスを一括してリポート可能となる。

【0225】このように、エンティティ単位でのリポートを実行することにより、1つ1つのデバイス単位で実行するリポート処理に比較して簡易なプロセスでのリポート処理が可能となる。

【0226】[エンティティのケイパビリティ管理] 次に、エンティティ単位でのキー配信ツリー構成において、各エンティティの許容するケイパビリティ (Capability) を管理して、ケイパビリティに応じたコンテンツ配信を行なう処理構成について説明する。ここでケイパビリティとは、例えば特定の圧縮音声データの復号が可能であるとか、特定の音声再生方式を許容するとか、あるいは特定の画像処理プログラムを処理できる等、デバイスがどのようなコンテンツ、あるいはプログラム等を処理できるデバイスであるか、すなわちデバイスのデータ処理能力の定義情報である。

【0227】図41にケイパビリティを定義したエンティティ構成例を示す。キー配信ツリー構成の最頂点にルートノードが位置し、下層に複数のエンティティが接続されて各ノードが2分岐を持つツリー構成である。ここで、例えばエンティティ4001は、音声再生方式A、B、Cのいずれかを許容するケイパビリティを持つエンティティとして定義される。具体的には、例えばある音声圧縮プログラム-A、B、またはC方式で圧縮した音楽データを配信した場合に、エンティティ4001以下に構成されたエンティティに属するデバイスは圧縮データを伸長する処理が可能である。

【0228】同様にエンティティ4002は音声再生方式BまたはC、エンティティ4003は音声再生方式AまたはB、エンティティ4004は音声再生方式B、エンティティ4005は音声再生方式Cを処理することが可能なケイパビリティを持つエンティティとして定義される。

【0229】一方、エンティティ4021は、画像再生方式p、q、rを許容するエンティティとして定義され、エンティティ4022は方式p、qの画像再生方式、エンティティ4023は方式pの画像再生が可能なケイパビリティを持つエンティティとして定義される。

【0230】このような各エンティティのケイパビリティ情報は、キー発行センター (KDC) において管理される。キー発行センター (KDC) は、例えばあるコンテンツプロバイダが特定の圧縮プログラムで圧縮した音楽データを様々なデバイスに配信したい場合、その特定の圧縮プログラムを再生可能なデバイスに対してのみ復号可能な有効化キーブロック (EKB) を各エンティティのケイパビリティ情報に基づいて生成することができる。コンテンツを提供するコンテンツプロバイダは、ケイパビリティ情報に基づいて生成した有効化キーブロッ

ク (EKB) によって暗号化したコンテンツキーを配信し、そのコンテンツキーで暗号化した圧縮音声データを各デバイスに提供する。この構成により、データの処理が可能なデバイスに対してのみ特定の処理プログラムを確実に提供することが可能となる。

【0231】なお、図41では全てのエンティティについてケイパビリティ情報を定義している構成であるが、図41の構成のようにすべてのエンティティにケイパビリティ情報を定義することは必ずしも必要ではなく、例えば図42に示すようにデバイスが属する最下段のエンティティについてのみケイパビリティを定義して、最下段のエンティティに属するデバイスのケイパビリティをキー発行センター (KDC) において管理して、コンテンツプロバイダが望む処理の可能なデバイスにのみ復号可能な有効化キーブロック (EKB) を最下段のエンティティに定義されたケイパビリティ情報に基づいて生成する構成としてもよい。図42では、末端ノードにデバイスが定義されたエンティティ4101=4105におけるケイパビリティが定義され、これらのエンティティについてのケイパビリティをキー発行センター (KDC) において管理する構成である。例えばエンティティ4101には音声再生については方式B、画像再生については方式rの処理が可能なデバイスが属している。エンティティ4102には音声再生については方式A、画像再生については方式qの処理が可能なデバイスが属している等である。

【0232】図43にキー発行センター (KDC) において管理するケイパビリティ管理テーブルの構成例を示す。ケイパビリティ管理テーブルは、図43(a)のようなデータ構成を持つ。すなわち、各エンティティを識別する識別子としてのエンティティID、そのエンティティに定義されたケイパビリティを示すケイパビリティリスト、このケイパビリティリストは図43(b)に示すように、例えば音声データ再生処理方式(A)が処理可能であれば[1]、処理不可能であれば[0]、音声データ再生処理方式(B)が処理可能であれば[1]、処理不可能であれば[0]…等、様々な態様のデータ処理についての可否を1ビットづつ[1]または[0]を設定して構成されている。なお、このケイパビリティ情報の設定方法はこのような形式に限らず、エンティティの管理デバイスについてのケイパビリティを識別可能であれば他の構成でもよい。

【0233】ケイパビリティ管理テーブルには、さらに、各エンティティのサブEKB、あるいはサブEKBが別のデータベースに格納されている場合は、サブEKBの識別情報が格納され、さらに、各エンティティのサブルートノード識別データが格納される。

【0234】キー発行センター (KDC) は、ケイパビリティ管理テーブルに基づいて、例えば特定のコンテンツの再生可能なデバイスのみが復号可能な有効化キーブ

51

ロック (EKB) を生成する。図44を用いて、ケイパビリティ情報に基づく有効化キープロックの生成処理について説明する。

【0235】まず、ステップS4301において、キー発行センター (KDC) は、ケイパビリティ管理テーブルから、指定されたケイパビリティを持つエンティティを選択する。具体的には、例えばコンテンツプロバイダが音声データ再生処理方式Aに基づく再生可能なデータを配信したい場合は、図43(a)のケイパビリティリストから、例えば音声データ再生処理 (方式A) の項目が [1] に設定されたエンティティを選択する。

【0236】次に、ステップS4302において、選択されたエンティティによって構成される選択エンティティIDのリストを生成する。次に、ステップS4303で、選択エンティティIDによって構成されるツリーに必要なパス (キー配信ツリー構成のパス) を選択する。ステップS4304では、選択エンティティIDのリストに含まれる全てのパス選択が完了したか否かを判定し、完了するまで、ステップS4303においてパスを生成する。これは、複数のエンティティが選択された場合に、それぞれのパスを順次選択する処理を意味している。

【0237】選択エンティティIDのリストに含まれる全てのパス選択が完了すると、ステップS4305に進み、選択したパスと、選択エンティティによってのみ構成されるキー配信ツリー構造を構築する。

【0238】次に、ステップS4306において、ステップS4305で生成したツリー構造のノードキーの更新処理を行ない、更新ノードキーを生成する。さらに、ツリーを構成する選択エンティティのサブEKBをケイパビリティ管理テーブルから取り出し、サブEKBと、ステップS4306で生成した更新ノードキーとに基づいて選択エンティティのデバイスにおいてのみ復号可能な有効化キープロック (EKB) を生成する。このようにして生成した有効化キープロック (EKB) は、特定のケイパビリティを持つデバイスにおいてのみ利用、すなわち復号可能な有効化キープロック (EKB) となる。この有効化キープロック (EKB) で例えばコンテンツキーを暗号化して、そのコンテンツキーで特定プログラムに基づいて圧縮したコンテンツを暗号化してデバイスに提供することで、キー発行センター (KDC) によって選択された特定の処理可能なデバイスにおいてのみコンテンツが利用される。

【0239】このようにキー発行センター (KDC) は、ケイパビリティ管理テーブルに基づいて、例えば特定のコンテンツの再生可能なデバイスのみが復号可能な有効化キープロック (EKB) を生成する。従って、新たなエンティティが登録される場合には、その新規登録エンティティのケイパビリティを予め取得することが必要となる。このエンティティ新規登録に伴うケイパビ

52

ティ通知処理について図45を用いて説明する。

【0240】図45は、新規エンティティがキー配信ツリー構成に参加する場合のケイパビリティ通知処理シーケンスを示した図である。

【0241】新たにツリー構成中に追加される新規 (子) エンティティ (N-En) は、上位 (親) エンティティ (P-En) に対して新規登録要求を実行する。なお、各エンティティは、公開鍵暗号方式に従った公開鍵を保有し、新規エンティティは自己の公開鍵を登録要求に際して上位エンティティ (P-En) に送付する。

【0242】登録要求を受領した上位エンティティ (P-En) は、受領した新規 (子) エンティティ (N-En) の公開鍵を証明書発行局 (CA: Certificate Authority) に転送し、CAの署名を付加した新規 (子) エンティティ (N-En) の公開鍵を受領する。これらの手続きは、上位エンティティ (P-En) と新規 (子) エンティティ (N-En) との相互認証の手続きとして行われる。

【0243】これらの処理により、新規登録要求エンティティの認証が終了すると、上位エンティティ (P-En) は、新規 (子) エンティティ (N-En) の登録を許可し、新規 (子) エンティティ (N-En) のノードキーを新規 (子) エンティティ (N-En) に送信する。このノードキーは、上位エンティティ (P-En) の末端ノードの1つのノードキーであり、かつ、新規 (子) エンティティ (N-En) の頂点ノード、すなわちサブルートキーに対応する。

【0244】このノードキー送信が終了すると、新規 (子) エンティティ (N-En) は、新規 (子) エンティティ (N-En) のツリー構成を構築し、構築したツリーの頂点に受信した頂点ノードのサブルートキーを設定し、各ノード、リーフのキーを設定して、エンティティ内の有効化キープロック (サブEKB) を生成する。一方、上位エンティティ (P-En) も、新規 (子) エンティティ (N-En) の追加により、有効化する末端ノードを追加した上位エンティティ (P-En) 内のサブEKBを生成する。

【0245】新規 (子) エンティティ (N-En) は、新規 (子) エンティティ (N-En) 内のノードキー、リーフキーによって構成されるサブEKBを生成すると、これを上位エンティティ (P-En) に送信し、さらに、自己のエンティティで管理するデバイスについてのケイパビリティ情報を上位エンティティに通知する。

【0246】新規 (子) エンティティ (N-En) からサブEKBおよびケイパビリティ情報を受信した上位エンティティ (P-En) は、受信したサブEKBとケイパビリティ情報と、上位エンティティ (P-En) の更新したサブEKBとをキー発行センター (KDC: Key Distribute Center) に送信する。

【0247】キー発行センター (KDC) は、受領した

53

エンティティのサブEKBおよびケイパビリティ情報とを図43で説明したケイパビリティ管理テーブルに登録し、ケイパビリティ管理テーブルを更新する。キー発行センター(KDC)は、更新したケイパビリティ管理テーブルに基づいて、様々な態様のEKB、すなわち特定のケイパビリティを持つエンティティあるいはデバイスのみが復号可能なEKBを生成することが可能となる。

【0248】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0249】

【発明の効果】以上、説明したように、本発明の情報処理システムおよび方法によれば、コンテンツキーや認証キー、コンテンツチェック値生成キー、プログラムデータ等の暗号化処理キープブロックとして適用可能な有効化キープブロック(EKB)の生成において、階層的鍵配信ツリーを配信デバイスに応じて再構築して、再構築した簡略ツリーに含まれるノード、リーフに基づいて有効化キープブロック(EKB)を生成する構成としたので、有効化キープブロック(EKB)の大幅なデータ量削減が実現される。

【0250】また、本発明の情報処理システムおよび方法によれば、簡略化した再構築階層ツリーに基づく有効化キープブロック(EKB)を構成し、さらに、EKB中の暗号化キーデータの位置識別子としてのタグに暗号化キーデータの有無を判別するデータを含ませた構成としたので、EKBの大幅なデータ量削減が実現されるとともに、EKBを受領したデバイスでのタグを用いた暗号化キーデータの抽出が容易となり、デバイスでのEKB復号処理が効率的になる。

【図面の簡単な説明】

【図1】本発明の情報処理システムの構成例を説明する図である。

【図2】本発明の情報処理システムにおいて適用可能な記録再生装置の構成例を示すブロック図である。

【図3】本発明の情報処理システムにおける各種キー、データの暗号化処理について説明するツリー構成図である。

【図4】本発明の情報処理システムにおける各種キー、データの配布に使用される有効化キープブロック(EKB)の例を示す図である。

【図5】本発明の情報処理システムにおけるコンテンツキーの有効化キープブロック(EKB)を使用した配布例と復号処理例を示す図である。

【図6】本発明の情報処理システムにおける有効化キープブロック(EKB)のフォーマット例を示す図である。

54

【図7】本発明の情報処理システムにおける有効化キープブロック(EKB)のタグの構成を説明する図である。

【図8】本発明の情報処理システムにおける有効化キープブロック(EKB)と、コンテンツキー、コンテンツを併せて配信するデータ構成例を示す図である。

【図9】本発明の情報処理システムにおける有効化キープブロック(EKB)と、コンテンツキー、コンテンツを併せて配信した場合のデバイスでの処理例を示す図である。

10 【図10】本発明の情報処理システムにおける有効化キープブロック(EKB)とコンテンツを記録媒体に格納した場合の対応について説明する図である。

【図11】本発明の情報処理システムにおける有効化キープブロック(EKB)と、コンテンツキーを送付する処理を従来の送付処理と比較した図である。

【図12】本発明の情報処理システムにおいて適用可能な共通鍵暗号方式による認証処理シーケンスを示す図である。

20 【図13】本発明の情報処理システムにおける有効化キープブロック(EKB)と、認証キーを併せて配信するデータ構成と、デバイスでの処理例を示す図(その1)である。

【図14】本発明の情報処理システムにおける有効化キープブロック(EKB)と、認証キーを併せて配信するデータ構成と、デバイスでの処理例を示す図(その2)である。

【図15】本発明の情報処理システムにおいて適用可能な公開鍵暗号方式による認証処理シーケンスを示す図である。

30 【図16】本発明の情報処理システムにおいて公開鍵暗号方式による認証処理を用いて有効化キープブロック(EKB)と、コンテンツキーを併せて配信する処理を示す図である。

【図17】本発明の情報処理システムにおいて有効化キープブロック(EKB)と、暗号化プログラムデータを併せて配信する処理を示す図である。

【図18】本発明の情報処理システムにおいて適用可能なコンテンツ・インTEGRITY・チェック値(ICV)の生成に使用するMAC値生成例を示す図である。

40 【図19】本発明の情報処理システムにおける有効化キープブロック(EKB)と、ICV生成キーを併せて配信するデータ構成と、デバイスでの処理例を示す図(その1)である。

【図20】本発明の情報処理システムにおける有効化キープブロック(EKB)と、ICV生成キーを併せて配信するデータ構成と、デバイスでの処理例を示す図(その2)である。

50 【図21】本発明の情報処理システムにおいて適用可能なコンテンツ・インTEGRITY・チェック値(ICV)をメディアに格納した場合のコピー防止機能を説明する

55

図である。

【図 22】本発明の情報処理システムにおいて適用可能なコンテンツ・インテグリティ・チェック値（ICV）をコンテンツ格納媒体と別に管理する構成を説明する図である。

【図 23】本発明の情報処理システムにおける階層ツリー構造のカテゴリ分類の例を説明する図である。

【図 24】本発明の情報処理システムにおける簡略化有効化キーブロック（EKB）の生成過程を説明する図である。

【図 25】本発明の情報処理システムにおける有効化キーブロック（EKB）の生成過程を説明する図である。

【図 26】本発明の情報処理システムにおける簡略化有効化キーブロック（EKB）（例 1）を説明する図である。

【図 27】本発明の情報処理システムにおける簡略化有効化キーブロック（EKB）（例 2）を説明する図である。

【図 28】本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成について説明する図である。

【図 29】本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成の詳細について説明する図である。

【図 30】本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成について説明する図である。

【図 31】本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成でのリザーブノードについて説明する図である。

【図 32】本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成での新規エンティティ登録処理シーケンスについて説明する図である。

【図 33】本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成での新規エンティティと上位エンティティの関係について説明する図である。

【図 34】本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成で用いるサブ EKB について説明する図である。

【図 35】本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成でのデバイスリポート処理について説明する図である。

【図 36】本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成でのデバイスリポート処理シーケンスについて説明する図である。

【図 37】本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成でのデバイスリポート時の更新サブ EKB について説明する図である。

【図 38】本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成でのエンティティリポー

56

ク処理について説明する図である。

【図 39】本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成でのエンティティリポート処理シーケンスについて説明する図である。

【図 40】本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成でのリポートエンティティと上位エンティティの関係について説明する図である。

【図 41】本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成でのケイパビリティ設定について説明する図である。

【図 42】本発明の情報処理システムにおける階層ツリー構造のエンティティ管理構成でのケイパビリティ設定について説明する図である。

【図 43】本発明の情報処理システムにおけるキー発行センター（KDC）の管理するケイパビリティ管理テーブル構成を説明する図である。

【図 44】本発明の情報処理システムにおけるキー発行センター（KDC）の管理するケイパビリティ管理テーブルに基づく EKB 生成処理フロー図である。

【図 45】本発明の情報処理システムにおける新規エンティティ登録時のケイパビリティ通知処理を説明する図である。

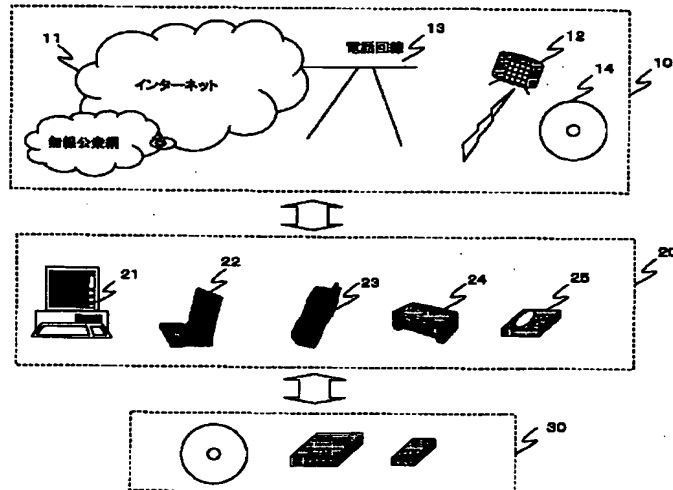
【符号の説明】

- 10 コンテンツ配信側
- 11 インターネット
- 12 衛星放送
- 13 電話回線
- 14 メディア
- 20 コンテンツ受信側
- 21 パーソナルコンピュータ（PC）
- 22 ポータブルデバイス（PD）
- 23 携帯電話、PDA
- 24 記録再生器
- 25 再生専用器
- 30 メディア
- 100 記録再生装置
- 110 バス
- 120 入出力 I/F
- 130 MPEG コーデック
- 140 入出力 I/F
- 141 A/D、D/A コンバータ
- 150 暗号処理手段
- 160 ROM
- 170 CPU
- 180 メモリ
- 190 ドライブ
- 195 記録媒体
- 601 バージョン
- 602 デプス

57

603 データポインタ
 604 タグポインタ
 605 署名ポインタ
 606 データ部
 607 タグ部
 608 署名
 1101 記録デバイス
 2301 ルートキー
 2302 ノードキー
 2303 リーフキー
 2304 カテゴリノード
 2306 サブカテゴリノード
 2701 エンティティ
 2702 サブルート
 2811, 2851 サブルート
 2812, 2852 エンティティ末端ノード
 2901, 2902 エンティティ
 2950 リザーブノード

【図1】



58

*2970 管理末端ノード
 3011, 3012, 3013 エンティティ
 3021, 3022, 3023 リザーブノード
 3201 末端ノード
 3202 頂点ノード
 3301, 3302 末端ノード
 3303 新規エンティティ追加末端ノード
 3410, 3420, 3430 エンティティ
 3411, 3421, 3431 サブルート
 10 3432 リボークデバイスノード
 3601 末端ノード
 3710, 3720, 3730 エンティティ
 3711, 3721, 3731 サブルート
 3901 末端ノード
 3902 頂点ノード (サブルートノード)
 4001~4005 エンティティ
 4021, 4022, 4023 エンティティ
 * 4101~4105 エンティティ

【図4】

(A) 有効化キーブロック(EKB:Enabling Key Block) 例1

デバイス0, 1, 2にバージョン:tのノードキーを送付

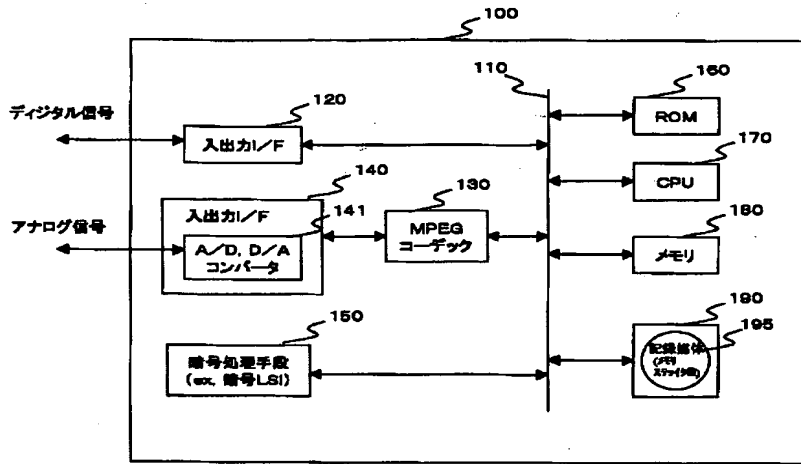
バージョン(Version):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

(B) 有効化キーブロック(EKB:Enabling Key Block) 例2

デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

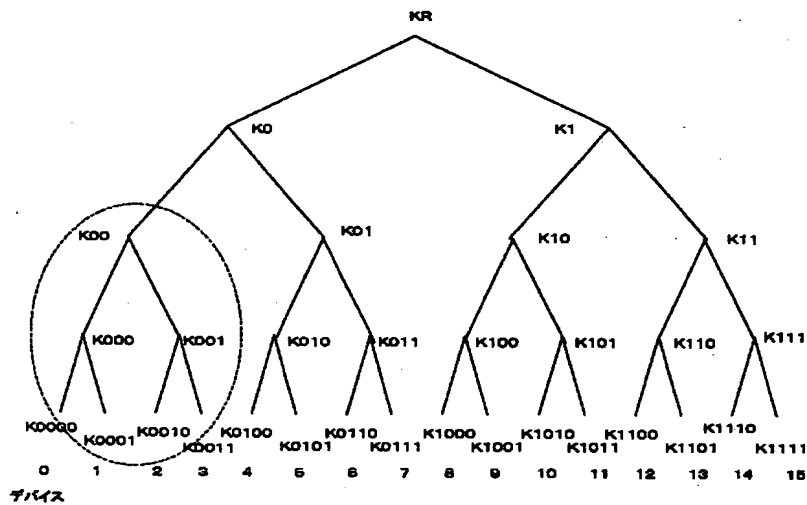
【図2】



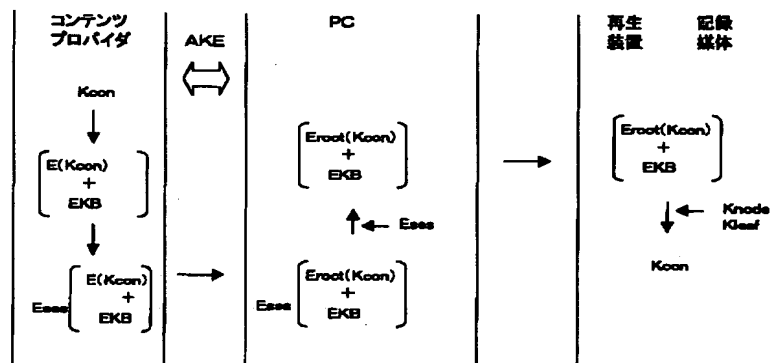
【図10】



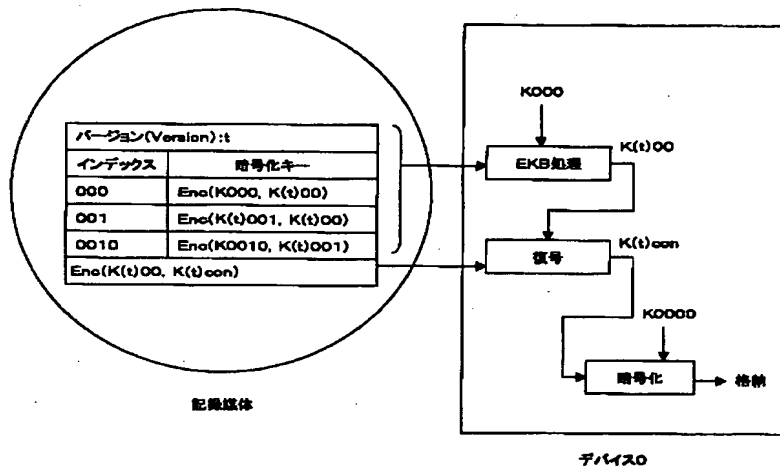
【図3】



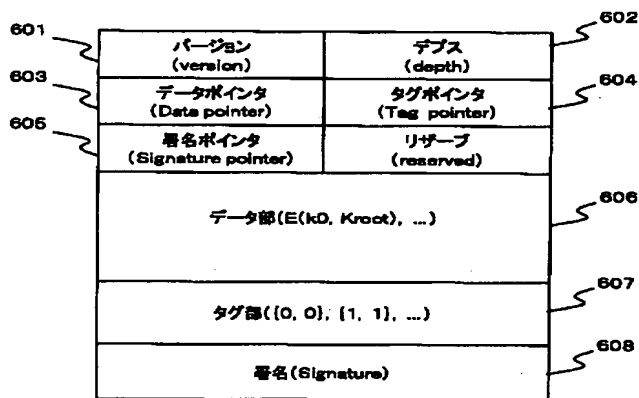
【図16】



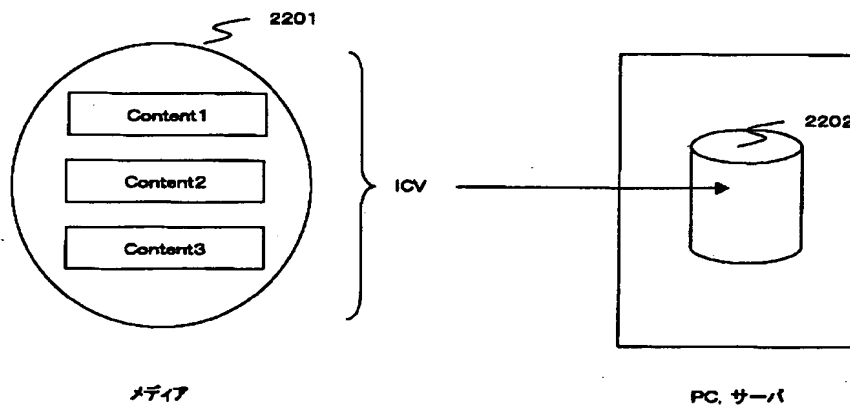
【図5】



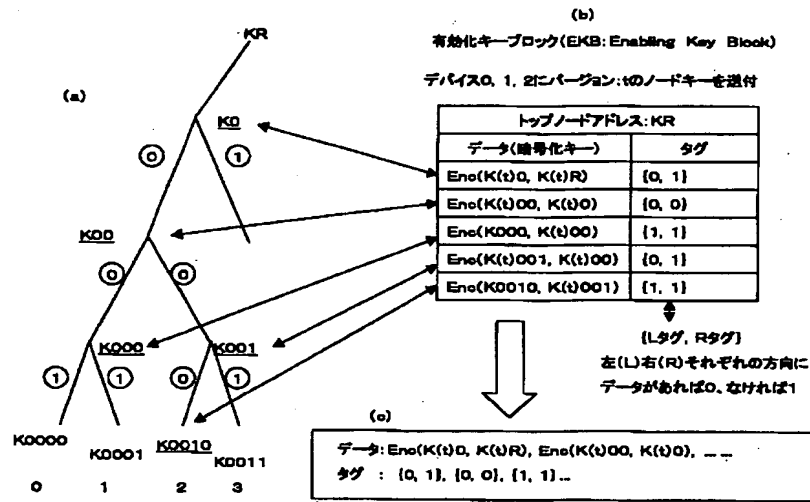
【図6】



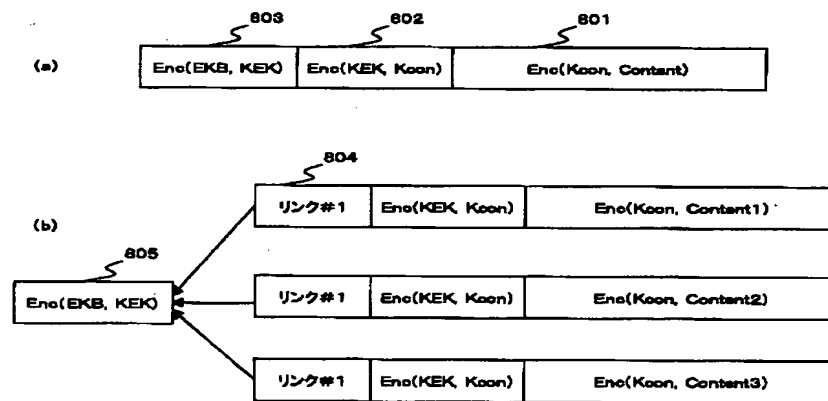
【図22】



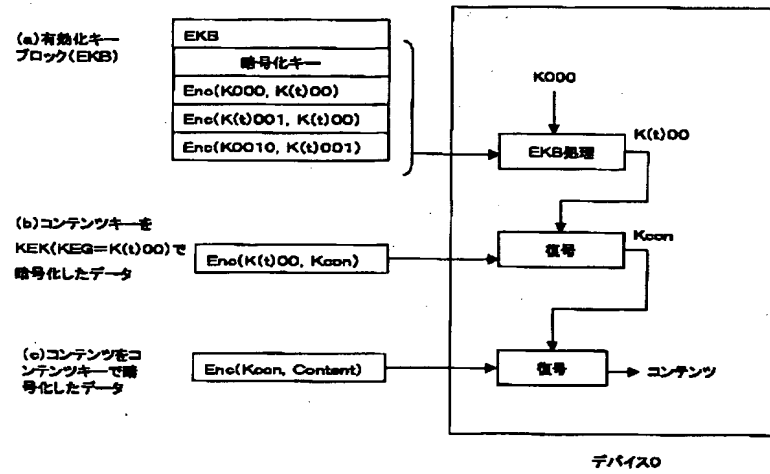
【図7】



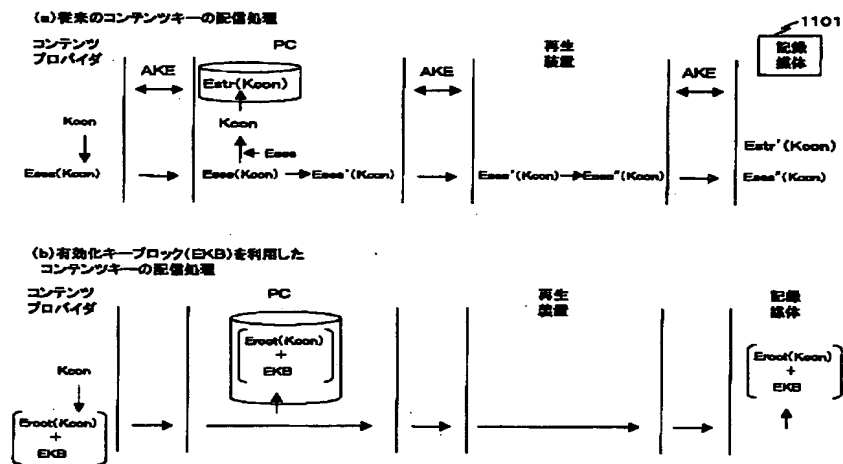
【図8】



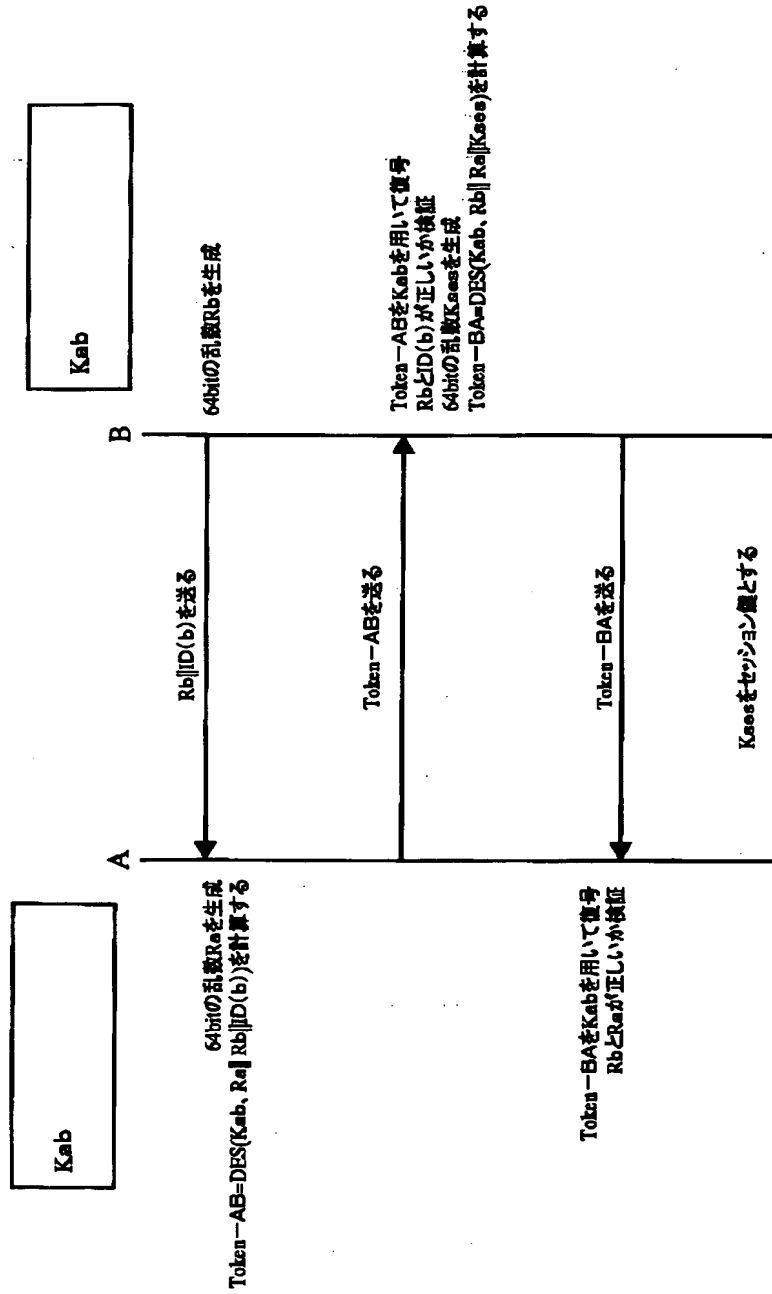
【図9】



【図11】

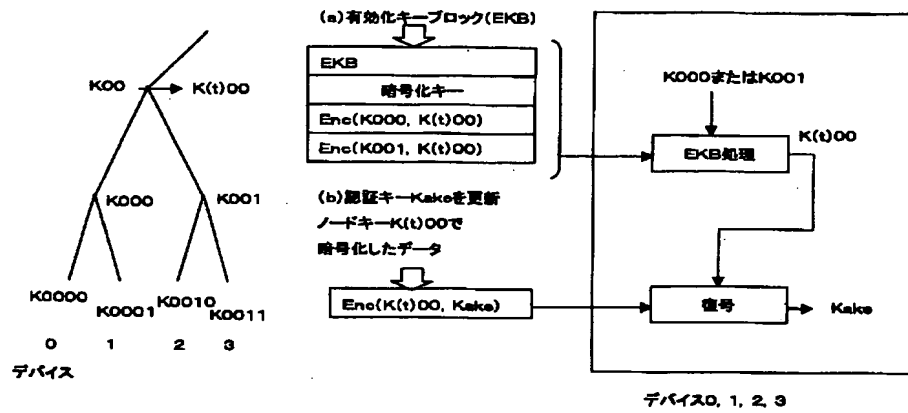


【図 12】

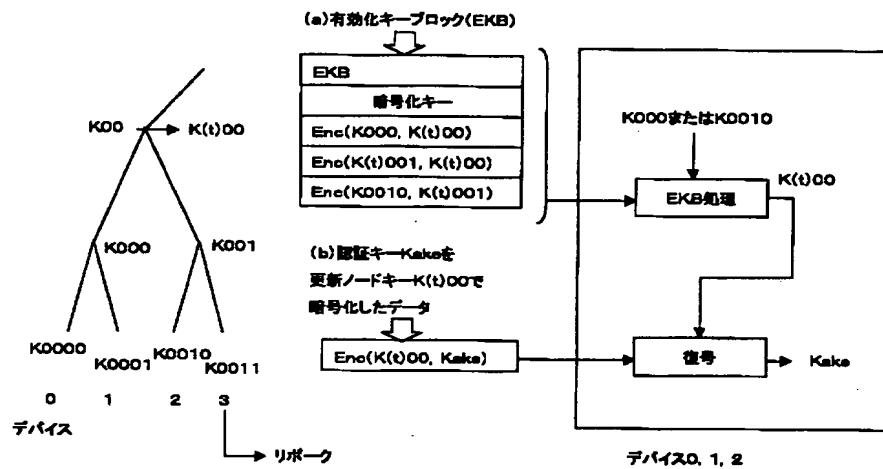


ISO/IEC 9798-2 対称鍵暗号技術を用いた相互認証および鍵共有方式

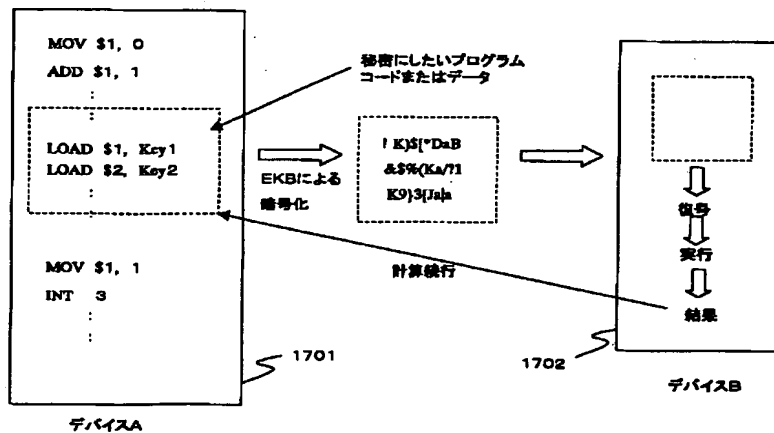
【図13】



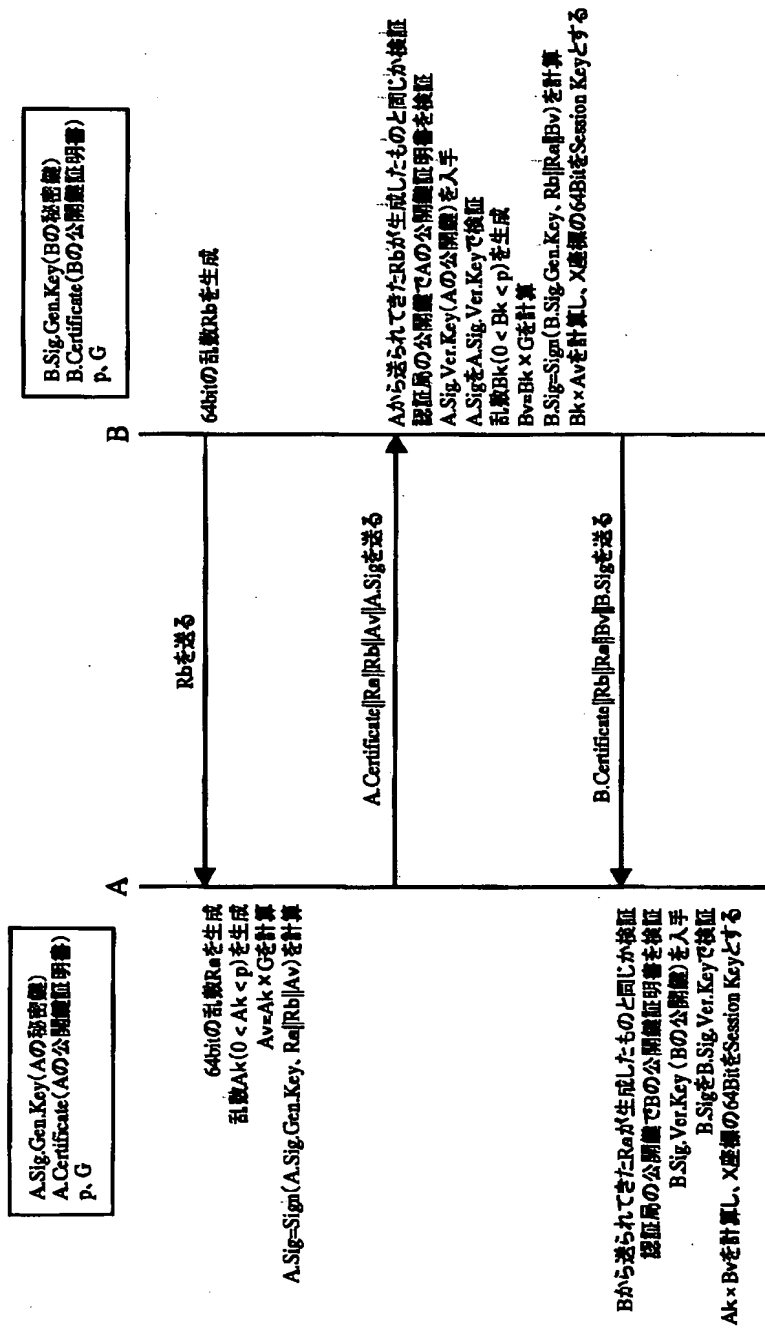
【図14】



【図17】

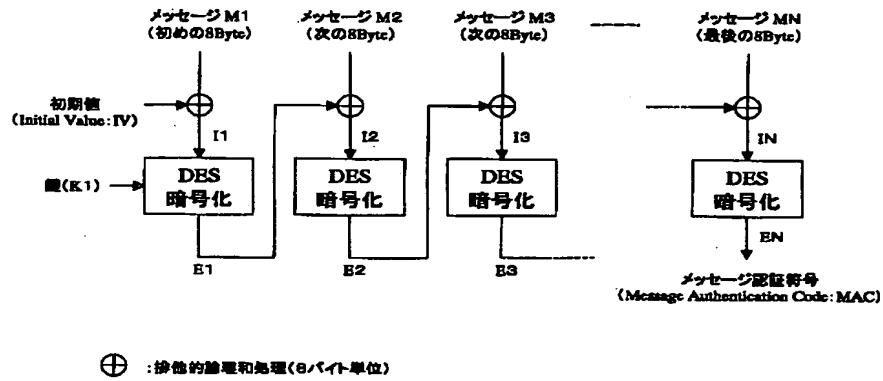


【図15】

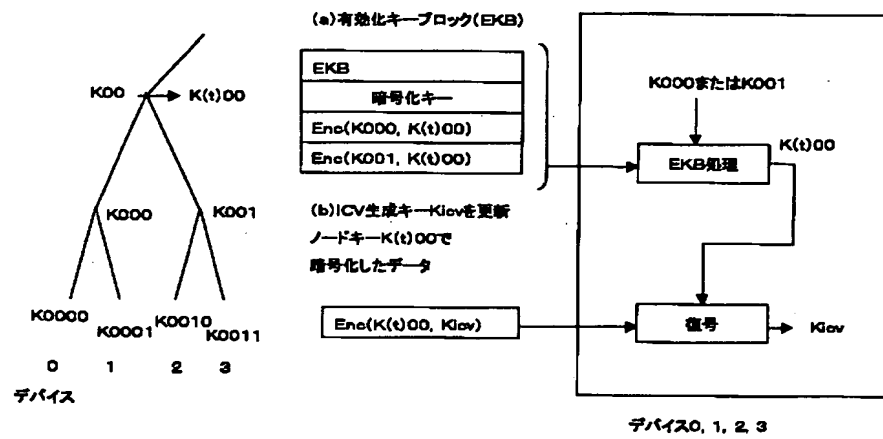


ISO/IEC 9798-3 非対称鍵暗号技術を用いた相互認証および鍵共有方式

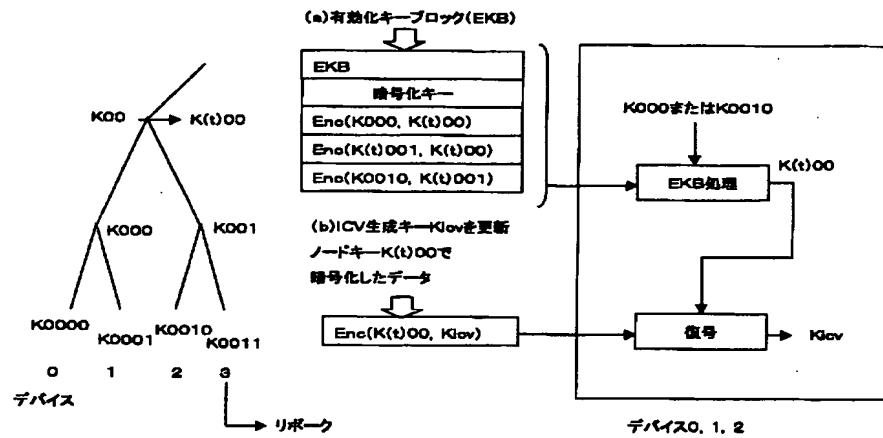
【図18】



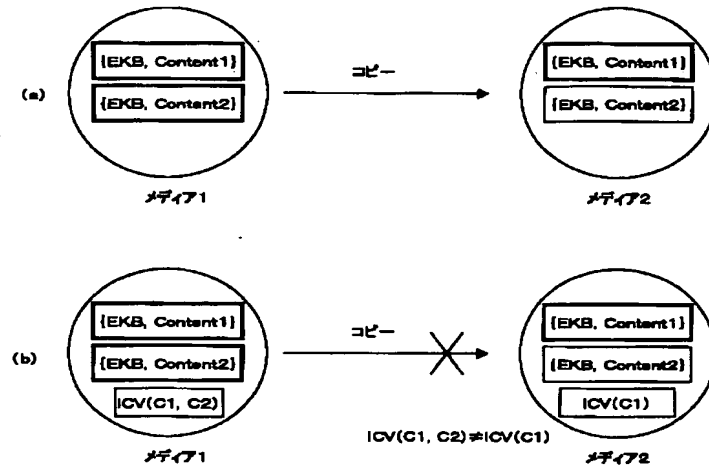
【図19】



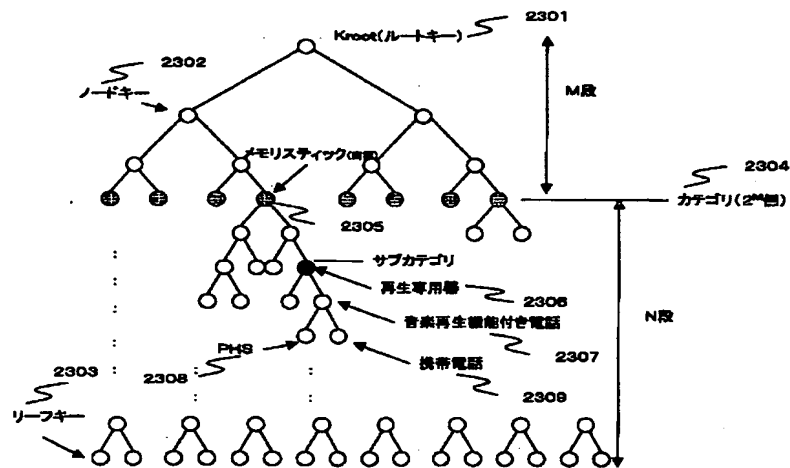
【図20】



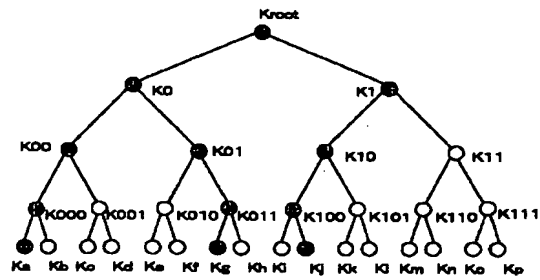
【図21】



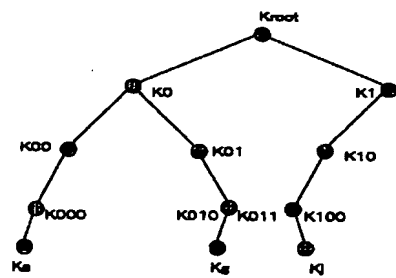
【図23】



【図24】

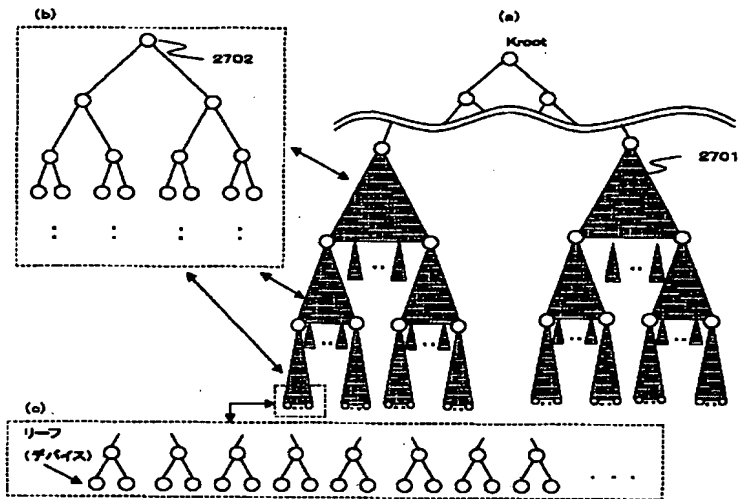


(a)



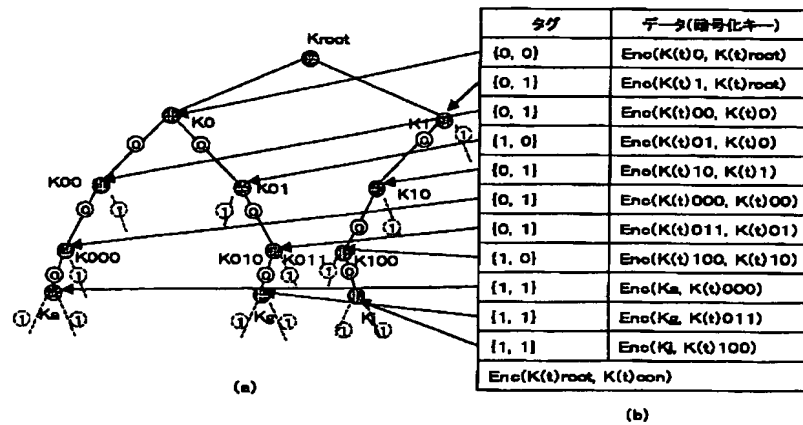
(b)

【図28】



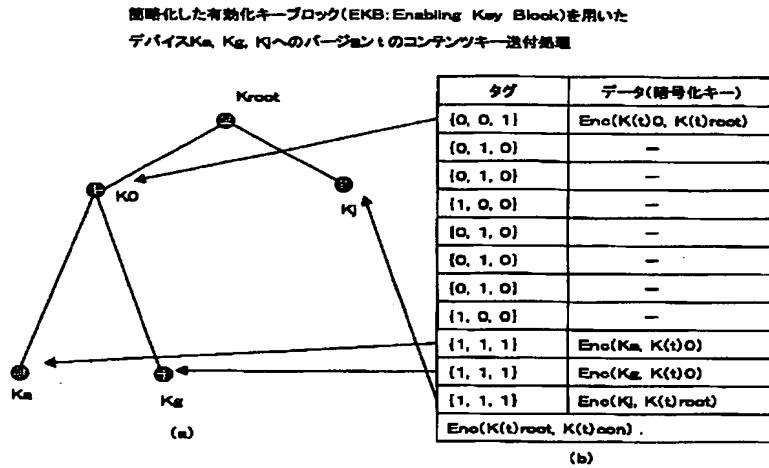
【図25】

有効化キーブロック(EKB: Enabling Key Block)を用いた
デバイスKa, Kg, Kiへのパージョン1のコンテンツキー送付処理

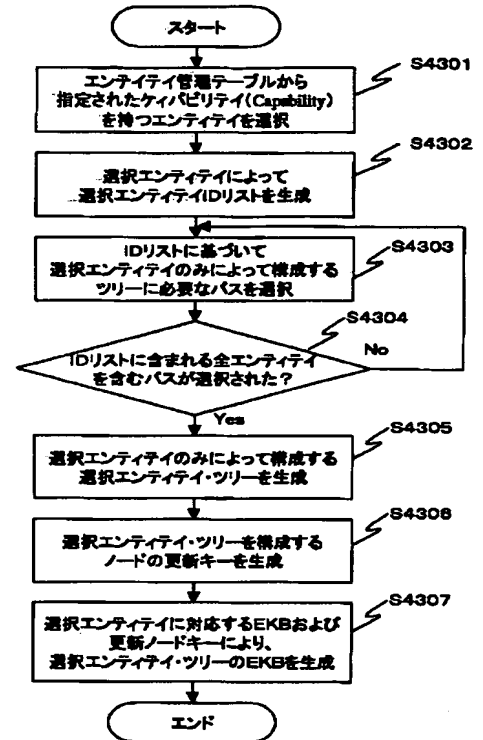


(b)

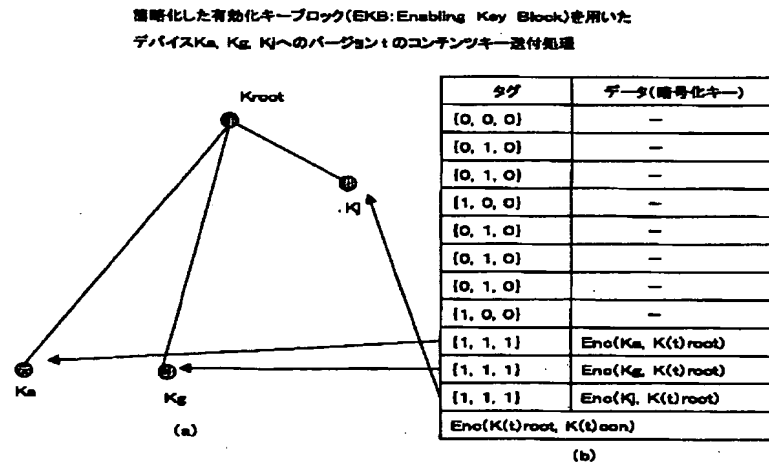
【図26】



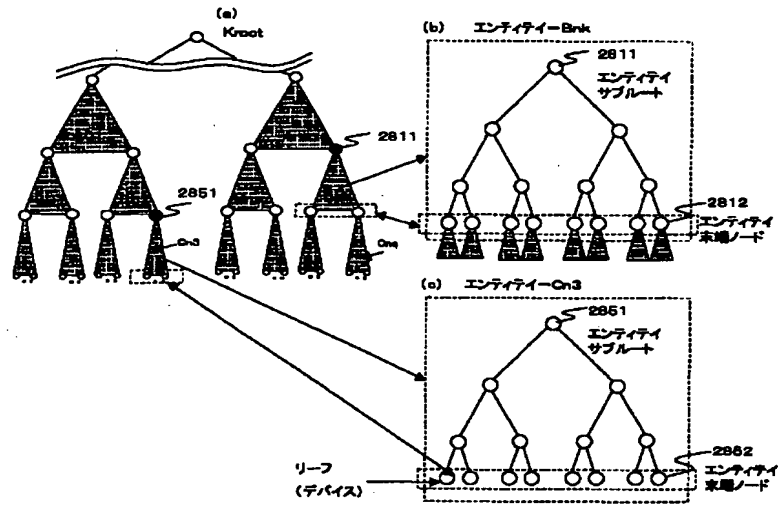
【図44】



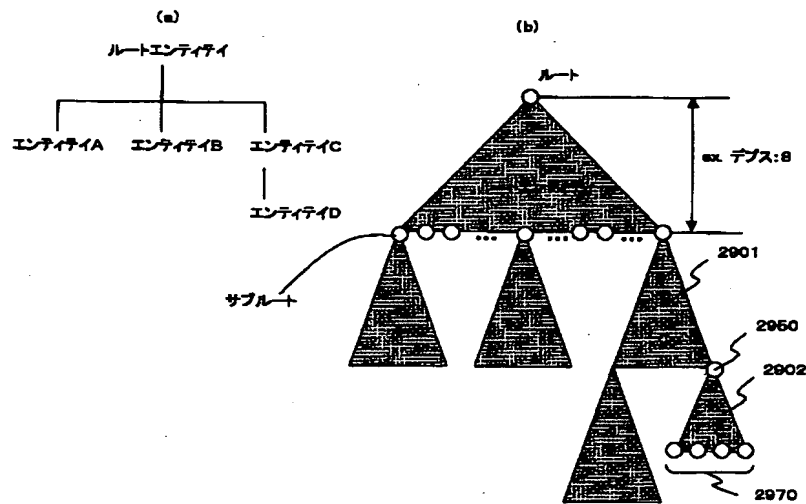
【図27】



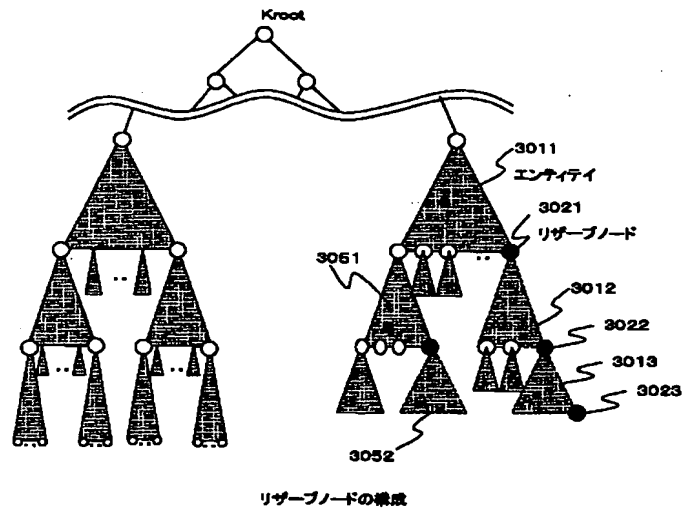
【図29】



【図30】

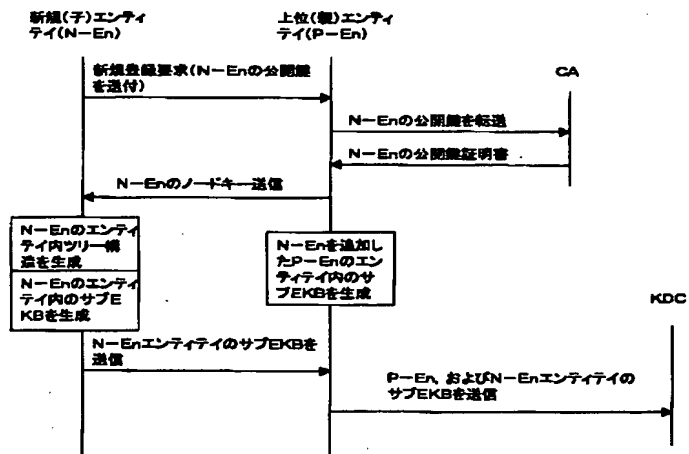


【図31】

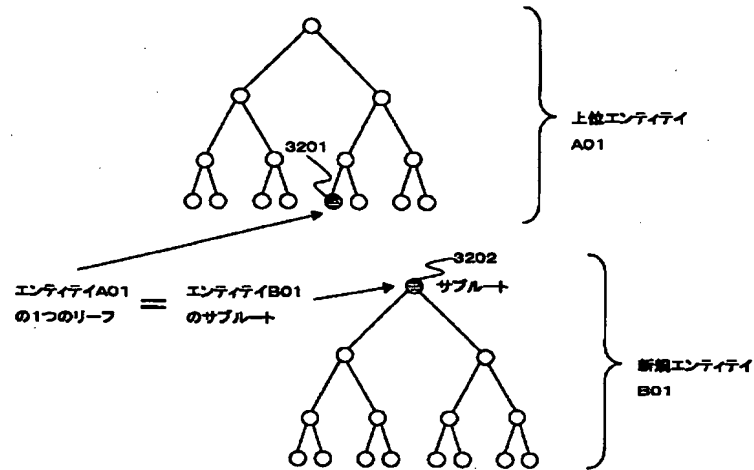


【図32】

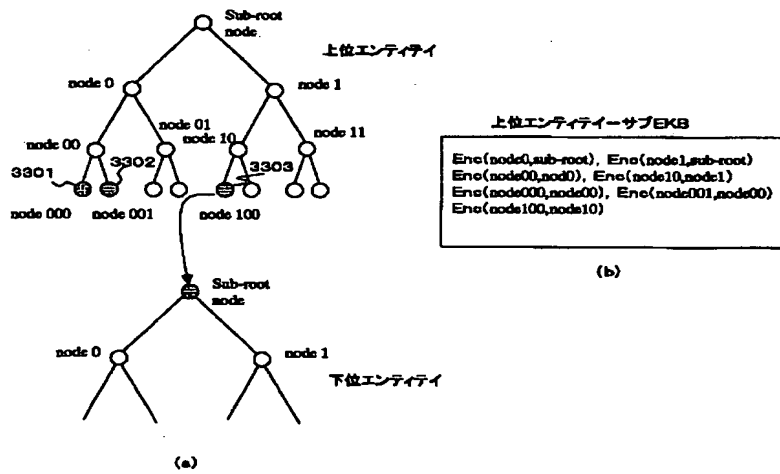
新規エンティティの登録処理



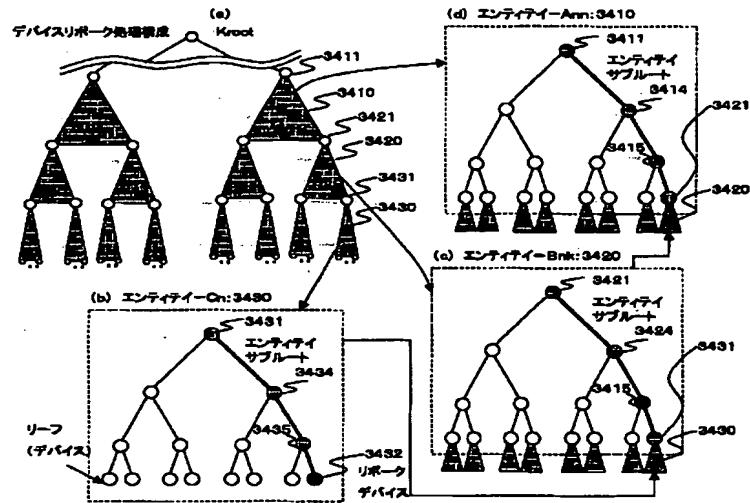
【図 33】



【図 34】

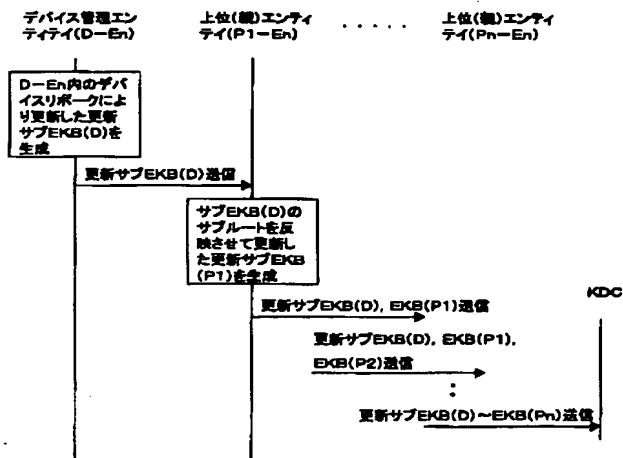


【図35】

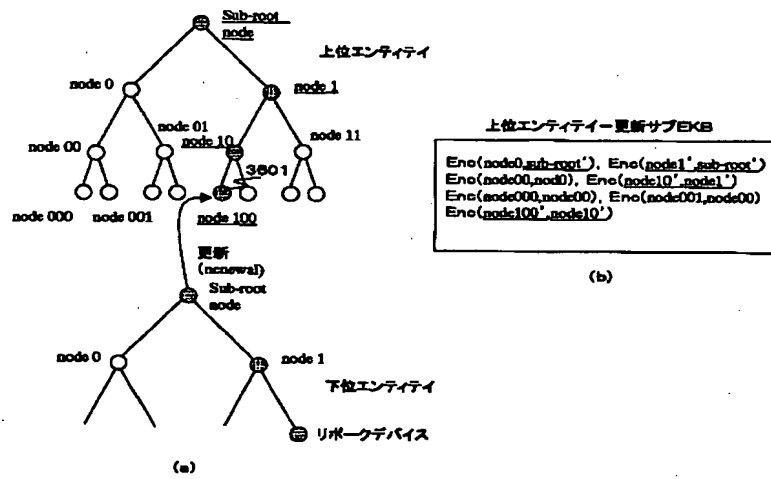


【図36】

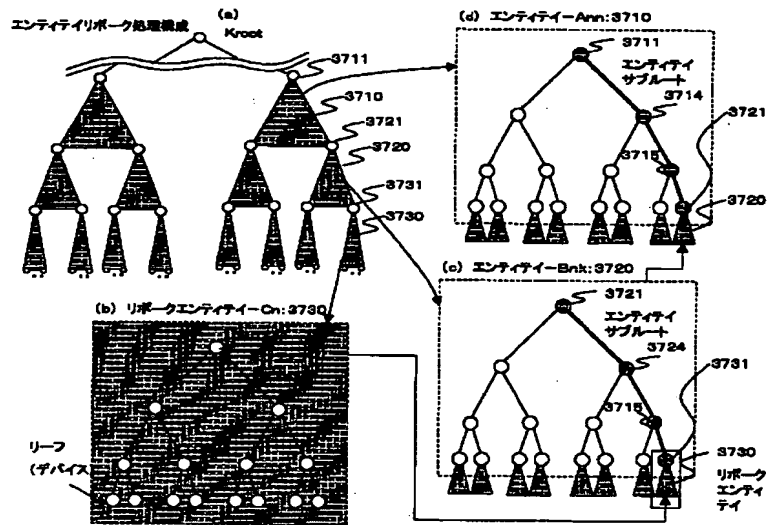
デバイスのリボーク処理



【図37】

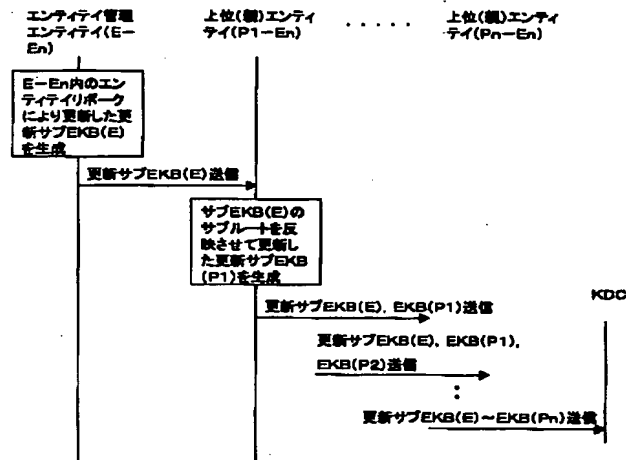


【図38】

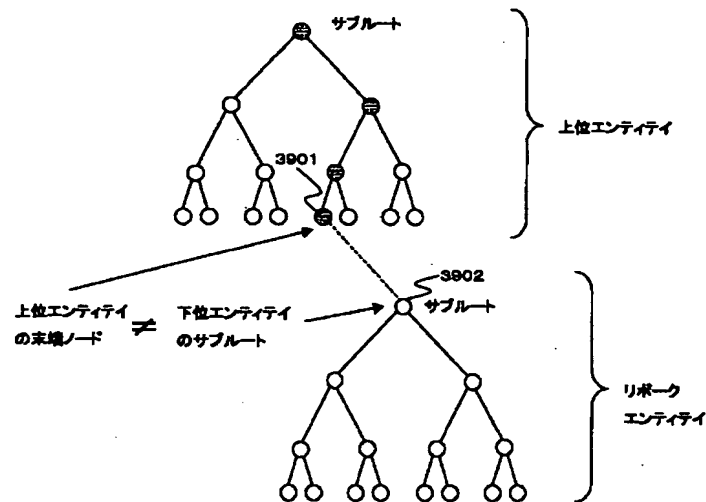


【図39】

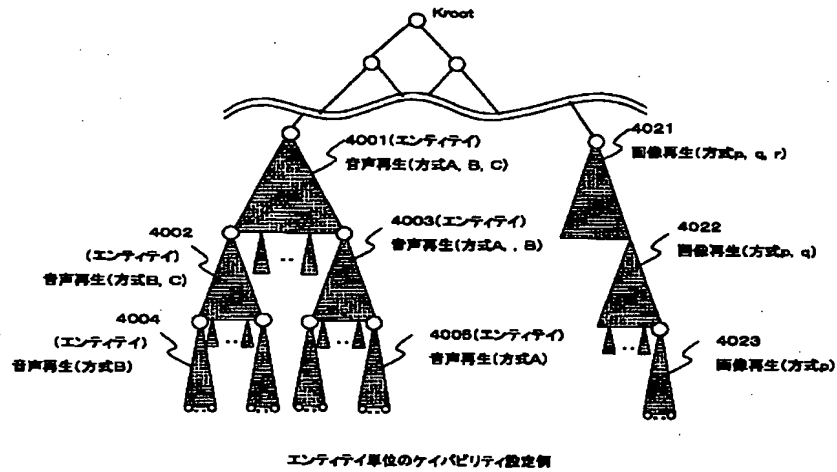
エンティティのリポート処理



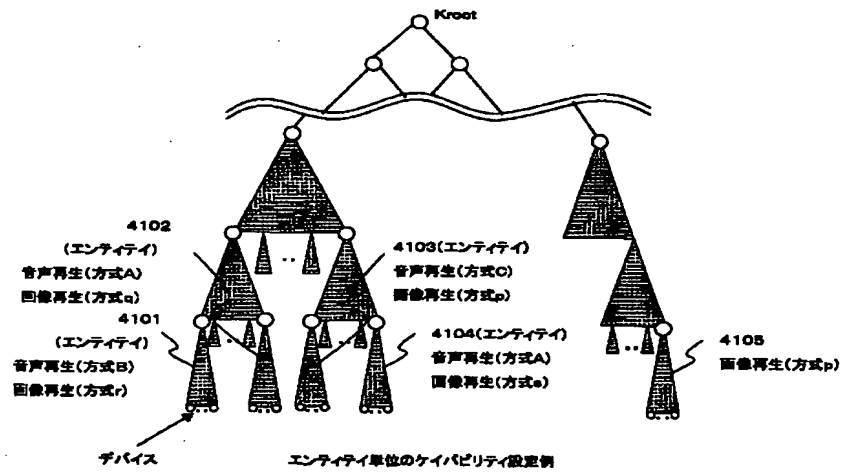
【図40】



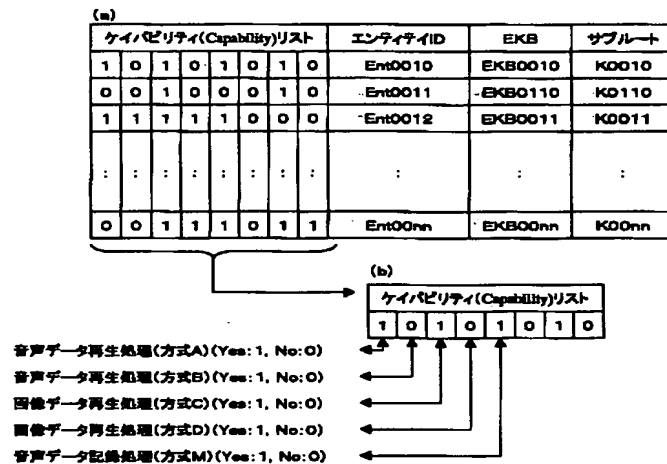
【図41】



【図42】

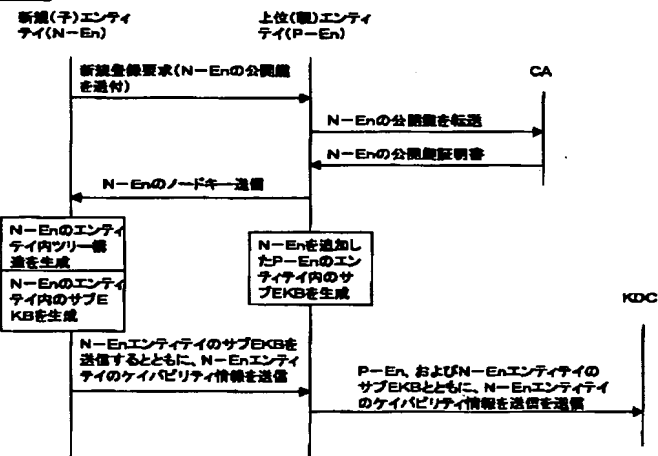


【図43】



【図45】

新規エンティティの登録処理に
伴うケイパビリティ通知



フロントページの続き

(72) 発明者 大石 文於
東京都品川区北品川 6 丁目 7 番 35 号 ソニ
ー株式会社内

(72) 発明者 浅野 智之
東京都品川区北品川 6 丁目 7 番 35 号 ソニ
ー株式会社内

(72) 発明者 光澤 敦
東京都品川区北品川 6 丁目 7 番 35 号 ソニ
ー株式会社内

F ターム (参考) 5J104 AA01 AA16 EA04 EA15 EA17
NA02 PA07

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.